

# Distributed Agency in AI-Enhanced Cybersecurity Education: A Posthuman Instructional Design Framework

Ryan Straight  
College of Information Science  
University of Arizona  
Tucson, AZ, USA  
ryanstraight@arizona.edu  
0000-0002-6251-5662

Josh Herron  
College of Arts and Humanities  
Clemson University  
Clemson, SC, USA  
jherron@clemson.edu  
0000-0001-5354-6785

**Abstract**—This paper addresses a critical challenge facing cybersecurity educators: preparing students for AI-enhanced practice environments where effective action emerges from human-AI collaboration rather than individual expertise. Traditional instructional design frameworks assume human-centered learning processes that inadequately address distributed agency realities in contemporary cybersecurity operations. Drawing on Adams and Thompson’s posthuman inquiry methodology, this analysis develops a comprehensive pedagogical framework consisting of four principles: (1) Design for the Assemblage, Not the Individual, (2) Cultivate Relationality and Response-ability, (3) Embrace Emergence, Messiness, and Indeterminacy, and (4) Posthuman Assessment Approaches. The framework provides concrete instructional design implications, including strategies for configuring human-AI learning relations, integrating AI literacies across cognitive, civic, creative, and critical dimensions, and developing assemblage-aware cybersecurity case studies. These design implications bridge theoretical posthuman concepts with practical curriculum implementation through the lens of curriculum-as-lived rather than curriculum-as-plan. Preliminary implementation observations from an undergraduate cybersecurity ethics course demonstrate how posthuman-designed scenarios enable students to develop comfort with complexity and distributed analysis. Student reflections reveal progression from seeking singular solutions to embracing multiple valid perspectives, suggesting effective cultivation of human-AI collaborative competencies. The framework equips cybersecurity educators with both theoretical foundations and actionable design strategies for preparing students for distributed agency practice environments.

**Keywords**—*distributed agency, artificial intelligence, cyber-security education, posthumanism, human-AI collaboration*

## I. INTRODUCTION

The integration of artificial intelligence into cyber operations has transformed cyber defense practice, creating distributed systems where agency emerges from complex interactions between human operators and AI systems [1]. However, cybersecurity education continues emphasizing individual skill development and human-centric problem-solving approaches that inadequately prepare students for AI-enhanced practice environments. This misalignment between educational practice and professional reality represents a critical challenge for cybersecurity educators seeking to prepare students for contemporary practice environments.

Posthumanism, as employed in this analysis, refers to a theoretical orientation that decenters human agency as the sole or primary driver of action, recognizing instead that effective practice emerges from networks of human and non-human actors including technologies, systems, and environments [2]. This perspective does not diminish human significance but rather situates human capabilities within broader assemblages where agency is distributed across multiple participants. For cybersecurity education, this reframing proves particularly relevant as contemporary practice increasingly depends on human-AI collaboration rather than individual expertise alone. This paper addresses the gap between current educational practice and emerging professional realities by developing a posthuman instructional design framework for cybersecurity education. Through theoretical development and preliminary implementation observations from undergraduate cybersecurity education, the analysis proposes how posthuman pedagogical principles can prepare students for human-AI collaborative practice while addressing ethical considerations in distributed decision-making systems. The framework addresses three key questions: (1) How can posthuman pedagogical principles inform cybersecurity education design? (2) What implementation patterns emerge when students engage with distributed agency concepts? (3) What institutional adaptations support this pedagogical approach?

## II. DISTRIBUTED AGENCY IN CYBERSECURITY PRACTICE

Distributed agency, rooted in actor-network theory and posthumanist scholarship, recognizes that effective action emerges from networks of human and non-human actors rather than individual agents [3]. Contemporary cybersecurity operations exemplify this through hybrid human-AI assemblages where security capabilities emerge from dynamic interactions between analysts, AI systems, automated mechanisms, and organizational protocols.

Modern Security Operations Centers (SOCs) demonstrate distributed agency across integrated domains. Threat detection involves machine learning algorithms processing thousands of security events per second while human analysts provide contextual interpretation and strategic assessment—neither component possesses complete detection capability independently. Response coordination integrates automated systems executing immediate containment actions with human operators managing broader incident strategies and stakeholder communication. Intelligence synthesis combines AI processing of vast data streams with human expertise interpreting patterns and strategic implications, producing insights that neither computational analysis nor human reasoning could achieve alone.

## III. LIMITATIONS OF TRADITIONAL INSTRUCTIONAL DESIGN

Traditional instructional design frameworks provide valuable foundations that continue to inform effective pedagogy, yet require significant adaptation to address distributed agency realities in cybersecurity education. These frameworks emerged from human-centered learning paradigms that have demonstrated substantial effectiveness in conventional educational contexts. However, distributed agency recognizes learning as emerging from networks of human and non-human actors, revealing specific limitations when applying traditional approaches to AI-enhanced learning environments.

Several foundational frameworks illustrate both enduring contributions and adaptation requirements. Vygotsky's [4] Zone of Proximal Development emphasizes how learners develop capabilities through guided interaction with more capable others—a concept that remains valuable but traditionally assumes human-to-human scaffolding rather than human-AI collaborative support. Similarly, Lave and Wenger's [5] situated learning theory positions learning within communities of practice, offering crucial insights about social learning contexts while focusing primarily on human communities rather than hybrid human-technology assemblages.

Contemporary instructional design models face parallel challenges. Merrill's First Principles [6] emphasize problem-centered learning yet assume individual learners engaging with static content, limiting applicability to dynamic human-AI interactions. While Gagné's Nine Events [7] provide systematic

lesson progression, they position the instructor as primary agent without accommodating multiple sources of agency. Kolb's Experiential Learning [8] offers valuable frameworks for processing experience through individual reflection, though it misses collaborative sense-making with AI systems. Problem-Based Learning [9] assumes human-only teams where AI is positioned as tools rather than collaborators, even as it involves authentic problems and sustained investigation.

These frameworks remain allied methods that provide essential pedagogical foundations. The challenge lies not in replacing these approaches but in extending them to accommodate the distributed nature of contemporary cybersecurity practice. This gap necessitates pedagogical approaches that integrate established principles with posthumanist understanding of agency distribution across human-AI networks.

## IV. POSTHUMAN INSTRUCTIONAL DESIGN FRAMEWORK

Given these limitations in traditional approaches, what is needed is a pedagogical framework that embraces rather than resists the distributed nature of contemporary cybersecurity practice. To address these educational limitations and prepare students for distributed agency practice, this analysis develops a comprehensive pedagogical framework grounded in posthuman theory. Building on Adams and Thompson's [10] posthuman inquiry methodology, this framework adapts their eight heuristics into four principles for cybersecurity education that incorporates distributed agency concepts. These principles address the gap between traditional human-centered instructional design and the network-based realities of contemporary cybersecurity practice. Figure 1 illustrates the fundamental topological distinction between these approaches.

### A. *Principle 1: Design for the Assemblage, Not the Individual*

This principle operationalizes Adams and Thompson's "Follow the Actors" and "Constructing Co(a)gents" heuristics by tracing how human and non-human elements co-constitute learning realities. The designer or learner is directed to trace how different human and non-human elements are brought together and how they co-constitute the realities in which learning occurs. This guides thinking of technology not as a tool, but in its embodied form as an integrated assemblage, precisely in the vein of postphenomenological technological relations [11].

The resultant instructional design departs from traditional human-centered learning and focuses instead on the holistic learning experience that emerges from interactions between human learners, AI systems, and the broader educational context. Rather than organizing curriculum around individual competencies, learning experiences are structured around network capabilities that emerge from human-AI collaboration, involving scenarios where students must coordinate with AI systems to achieve security objectives.

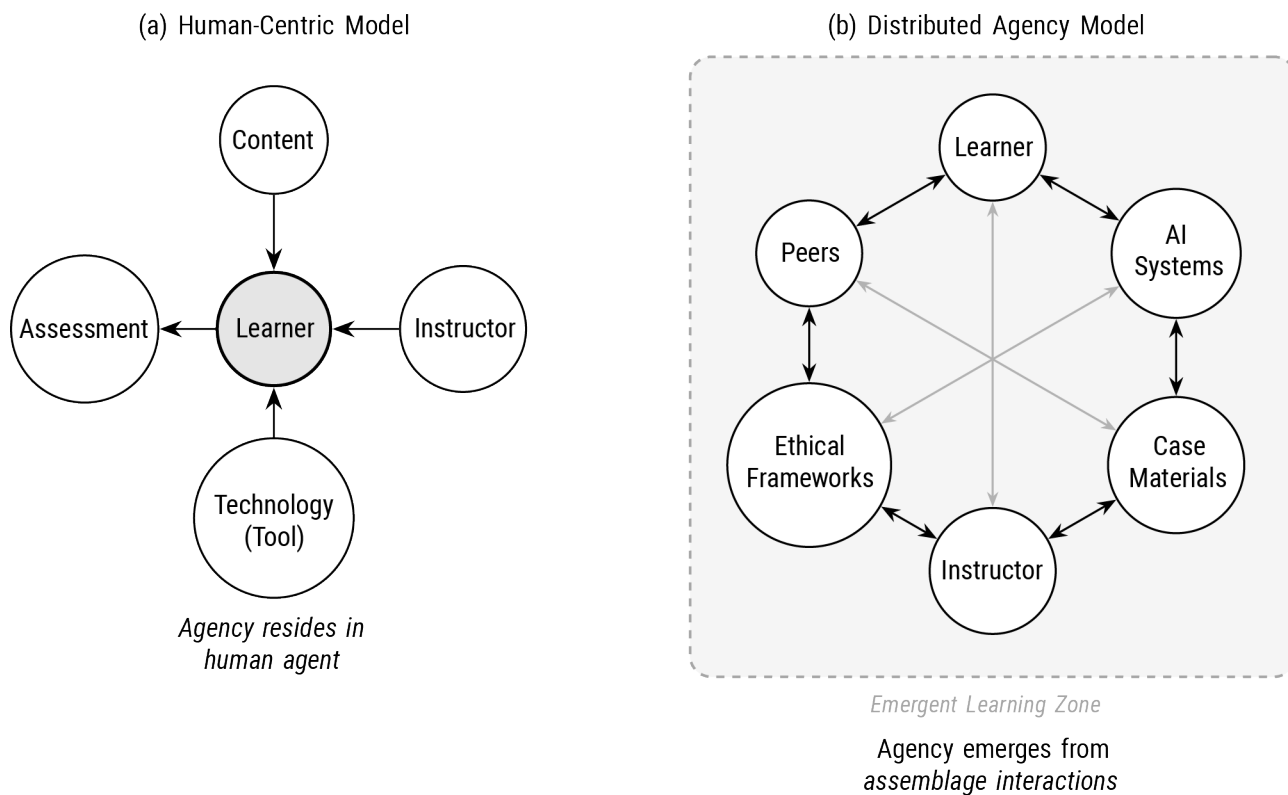


Fig. 1. Comparison of instructional design topologies. (a) Human-centric models position the learner as central agent receiving content and producing assessable outputs. (b) Distributed agency models recognize learning as emerging from networked interactions among human and non-human actors, with no privileged center.

### B. Principle 2: Cultivate Relationality and Response-ability

The second principle addresses the ethical orientation and considerations of posthuman instructional design, specifically engaging the quality of relationships between all actants in the assemblage. As posthuman inquiry leads to an inherently ethical stance by treating humans and technologies as legitimate participants in a given process, there is inherently established relationality. As with actor-network theory, entities are co-constituted by their relationships.

Through this process, learners are invited to become sensitive to how their perceptions are actively engaged and altered by the tools and technologies they engage. By attuning to these processes, learners gain key insights into more-than-human relationality and are invited to apply this understanding in their own learning and professional practice.

### C. Principle 3: Embrace Emergence, Messiness, and Indeterminacy

This principle establishes an epistemological shift through the application of posthumanist ideas. Traditional, human-centered epistemology is characterized by predictable, linear learning paths, whereas a posthumanist approach refocuses on emergent, complex, and “messy” processes of becoming. By aligning with these unpredictable pathways, educational

design can focus efforts on the process rather than predetermined results, studying *becoming* rather than *being*.

Posthuman inquiry heuristics focused on analyzing translations and studying breakdowns reframe failures and mistakes: they unveil the normally invisible work of non-human actors rather than serving as mere errors to correct. This reframing enables fuller ability to unravel the complex and sometimes contradictory environments in which learning is manifest.

### D. Principle 4: Posthuman Assessment Approaches

Though Adams and Thompson’s posthuman inquiry does not explicitly provide a roadmap for assessment, it provides a blueprint for what posthuman assessment might look like. An assignment might not instruct students to “solve the problem” or “debug the code,” but rather to “analyze the assemblage that made possible this predicament.” This could lead to evaluations that require students to examine how objects and technologies exist as integral and necessary parts of situations, and crucially, how agency can be attributed to them within the context of the assemblage.

Traditional assessment methods focused on individual performance inadequately evaluate distributed competencies. Collaborative performance assessment can evaluate student-

AI team outcomes rather than individual work. Process documentation asks students to articulate how they coordinate with AI systems across an analysis task. Adaptive response evaluation tests capacity to adjust strategies based on AI system feedback and changing conditions.

## V. INSTRUCTIONAL DESIGN IMPLICATIONS

The four posthuman principles carry direct implications for how instructional design is practiced. They shift how we think about the work of design itself. If a learning experience is already an assemblage of humans, machines, and systems, then design cannot be treated as a linear plan. It is a practice of configuring relations, bringing students, faculty, and AI systems into conditions for co-learning.

Japanese Canadian curriculum scholar Ted Aoki distinguished between curriculum-as-plan, the official and structured version, and curriculum-as-lived, the messy and relational reality of learning [12]. This distinction resonates with posthuman design principles. Traditional design reflects curriculum-as-plan: prescriptive and human-controlled. In practice, curriculum is always lived and relational. What appears neat on paper is enacted in shifting human-AI networks across policy, technologies, and materials. Posthuman instructional design leans into this lived dimension. Intentionality is not abandoned but redirected to cultivating conditions where learners act responsibly with nonhuman collaborators.

Because AI influences the relations that structure learning environments, assemblage thinking and curriculum-as-lived make AI literacies integral to design. Building on Doug Belshaw's *Digital Literacies*, AI literacies describe how humans learn *with* and *through* AI across eight dimensions: cognitive, civic, creative, critical, confident, cultural, communicative, and constructive [13], [14]. Framed in the plural, AI literacies capture the fact that learning with AI always involves multiple practices at once: reasoning, judging, creating, and communicating in relation to specific communities and contexts. At their core, they join skillsets (what people do with AI) with mindsets (how people approach AI).

TABLE I. Mapping of Posthuman Instructional Design Principles to AI Literacies

Posthuman Principle	AI Literacy	Design Focus
Design for the Assemblage	Cognitive	Understanding how AI processes and produces
Cultivate Relationality	Civic	Ethical entanglements with AI systems
Embrace Emergence	Creative	AI as generative partner
Posthuman Assessment	Critical	Interrogating outputs and biases

The four posthuman principles outlined in this paper align most closely with four of the eight literacies, as summarized in Table I. Designing for the assemblage emphasizes cognitive literacies, understanding how AI processes and produces. Cultivating relationality highlights civic literacies, foregrounding ethical entanglements with systems. Embracing emergence draws on creative literacies, treating AI as a generative partner. Posthuman assessment depends on critical literacies, interrogating outputs, assumptions, and biases. These literacies rarely appear in isolation but cluster in constellations, underscoring that instructional design cannot reduce human-AI learning to a single competency but must account for the plural and relational ways literacies are enacted together [14].

In practice, this mapping of literacies highlights specific ways instructional designers can build assemblage-aware cybersecurity learning. One strategy is designing incident case studies where AI tools are visible participants. Students might analyze threat detection reports generated by machine learning alongside human-authored documentation, tracing how decisions emerge from human-AI interactions. Assignments can ask learners to compare their analysis with AI-generated outputs, debate the ethical stakes of automated responses, and document where breakdowns or surprises surface. Such designs reflect curriculum-as-lived and cultivate literacies across cognitive, civic, creative, and critical dimensions.

From a posthuman perspective, design itself becomes a literacies practice. It develops the capacity to see, shape, and live within human-AI networks that characterize cybersecurity work. The goal is not only to prepare students to use AI, but to co-learn with it, working directly within the more-than-human systems that shape the field.

## VI. IMPLEMENTATION CONTEXT: DISTRIBUTED AGENCY IN UNDERGRADUATE CYBERSECURITY EDUCATION

While these four principles provide a theoretical foundation for posthuman instructional design, their practical application requires translation into concrete educational contexts. To further this framework, what follows are preliminary observations from implementing these posthuman instructional design principles within an undergraduate cybersecurity ethics course. These observations illustrate how the four principles can inform educational content creation and student learning experiences while revealing adaptation considerations for broader cybersecurity education enhancement. The observations below derive from a 15-week undergraduate cybersecurity ethics course ( $n=31$  students) that utilized case studies designed using posthuman principles embedded within complex, interconnected scenarios. Students worked in collaborative groups analyzing realistic cybersecurity scenarios that embodied distributed agency concepts through their narrative structure and stakeholder complexity. Course design emphasized how posthuman-informed content could create assemblage-aware learning experiences where students encountered multiple

perspectives and ethical frameworks simultaneously. This analysis presents observations from instructional practice; student reflections were collected as standard course feedback on case study materials. No personally identifiable information is disclosed, and quoted material has been anonymized to protect student privacy.

#### A. *Pedagogical Foundation and Demonstration Context*

Insofar as the use of case studies goes in cyber education, there tends to be an emphasis in technical skills and linear, predigested case analysis, inadequately preparing students for contemporary practice environments where ethical dilemmas emerge from complex networks of human and technological actors. Rather than positioning scenarios as isolated technical problems (i.e., a security breach at a water company), the posthuman instructional design framework embeds distributed agency concepts within case study narratives, creating educational contexts that reflect the complexity of professional practice realities. These cases provide accessible entry points for educators seeking to embed posthuman concepts within traditional cybersecurity education while illustrating how theoretical principles can inform practical curriculum design, leveraging real-world qualities like involving multiple stakeholders, conflicting perspectives, and distributed decision-making processes.

Case studies were delivered through a web-based digital textbook platform, providing students with fully online access to interconnected scenarios and supporting materials. In implementation contexts, students work in collaborative groups analyzing realistic cybersecurity incidents through authentic artifacts including technical documentation, communications, regulatory materials, and media coverage. Rather than approaching these materials through individual analysis, students engage in collaborative sense-making that mirrors the distributed nature of the scenarios themselves. The learning context that emerges includes student groups, complex case materials, multiple ethical frameworks, and instructor facilitation of discussions that embrace the inherent complexity and ambiguity of the scenarios.

Distributed agency principles manifest through the case study design itself, which embodies posthuman pedagogical concepts. Students encounter scenarios where agency is distributed across multiple actors—technical systems, organizational policies, individual decisions, and regulatory frameworks—requiring them to analyze situations that cannot be reduced to simple individual choice. As one student group reflected on their analytical approach: “One of our biggest strengths was how we applied multiple ethical frameworks. We used utilitarianism, deontology, and virtue ethics to look at the case from different angles instead of just sticking to one side... It’s easy to pick a side, but doing this gave us a better way to approach ethical case studies.” The foundation for this pedagogical approach emerges from sustained semester-length implementation utilizing multiple interconnected case studies that enable students to develop comfort with

complexity and distributed analysis impossible in isolated exercises.

The distributed agency approach creates sustained student-AI partnerships through collaborative analysis of complex cybersecurity scenarios requiring integration across multiple domains. Preliminary observations from course implementation reveal learning patterns that align with posthuman theoretical predictions about engaging with complex, distributed scenarios. Early semester interactions typically showed students seeking singular, correct answers within the multifaceted case studies. However, as students progressed through interconnected scenarios, they began developing comfort with complexity and multiple valid perspectives. One student group reflected on a case regarding whistleblowing: “Our initial in-class discussions helped us form the foundation of our analysis by surfacing immediate questions. . . This caused us to have to analyze closely and were able to find that in different ethical frameworks, the actions could be considered right.” This progression demonstrates the cultivation of relationality and comfort with emergence that posthuman pedagogy seeks to develop.

This development extends beyond instrumental skill building to epistemological shifts in cybersecurity understanding that align with posthuman theoretical frameworks. Rather than viewing cybersecurity dilemmas as technical problems with clear solutions, students develop appreciation for security as emerging from complex networks of human decisions, technological capabilities, organizational policies, and regulatory frameworks. This perspective reflects distributed ontologies where ethical reasoning must account for agency distributed across multiple actors rather than focusing solely on individual choice [2].

This semester-long engagement with complex, posthuman-designed scenarios exemplifies the construction of co(a)gents, where students and the embedded technological concepts within the cases become mutually constituted through sustained analysis [10]. This process involves students developing understanding not only of how to approach cybersecurity problems through multiple perspectives but also of their own analytical capabilities when confronting irreducible complexity. As one student group noted: “One aspect of deontology is treating people as an end not a means to an end. We found that that aspect could be used to support open source. . . We also found that it could support the other side.” The co-constitution process reveals how students develop competencies not merely in technical analysis, but in engaging with the distributed nature of cybersecurity practice itself. Through sustained interaction with scenarios designed using posthuman principles, students learn to work with rather than against complexity and ambiguity. This exemplifies the “becoming-with” that characterizes authentic engagement with the complex sociotechnical nature of cybersecurity practice [15].

### B. Implementation Challenges and Strategic Lessons

Implementation reveals patterns that inform broader cybersecurity education enhancement. The evidence demonstrates how distributed agency principles scale from micro-interactions to systemic educational change while revealing predictable challenges and effective adaptation strategies.

Student progression patterns reveal development phases that align with posthuman theoretical understanding of subject formation through technological relations. Initial resistance to AI collaboration reflects modernist assumptions about autonomous human subjectivity, while gradual recognition of AI capabilities demonstrates what posthumanist scholars describe as the decentering of humanist assumptions about individual agency [16]. The eventual integration of human-AI collaboration as core competency represents successful cultivation of posthuman subjectivity that recognizes itself as always-already constituted through technological relations.

This progression requires sustained exposure rather than isolated experiences, suggesting that distributed agency pedagogy achieves optimal effectiveness through prolonged “becoming-with” processes that allow for the gradual reconfiguration of human-technology relations [15]. The temporal dimension proves critical not merely for skill development but for the ontological transformation that posthuman pedagogy seeks to cultivate: the recognition that human capabilities *emerge* through technological collaboration.

Professional development needs encompass posthuman pedagogical theory, assessment approaches for distributed performance, and critically, the capacity to embrace the messiness of posthuman educational assemblages [10]. Faculty must cultivate deep understanding of AI system capabilities and limitations, not merely as technical specifications but as collaborative partners with distinct epistemological approaches.

Institutional adaptation presents systemic challenges that extend beyond individual course modifications. Assessment policy frameworks require substantial revision to accommodate assemblage evaluation rather than individual performance measurement, while existing academic integrity policies need updating to distinguish between inappropriate AI dependence and legitimate human-AI collaboration. Infrastructure investments must support AI-integrated learning environments while maintaining educational technology standards, creating resource allocation challenges for institutions with limited technical capacity.

Curriculum approval processes typically assume individual-centered competency frameworks and may resist approaches that emphasize emergent, relational learning outcomes. Institutions must develop nuanced policies that require sophisticated understanding of pedagogical goals and collaborative learning processes.

### VII. FUTURE DIRECTIONS AND RESEARCH OPPORTUNITIES

The distributed agency framework for cybersecurity education opens multiple interconnected avenues for research, development, and broader educational transformation that extend beyond cybersecurity into other domains where human-AI collaboration is becoming essential. Systematic evaluation of distributed agency educational approaches requires longitudinal studies tracking graduate outcomes, employer satisfaction, and professional performance metrics. Research should examine whether students who experience distributed agency pedagogy demonstrate superior collaborative capabilities, adaptive problem-solving skills, and resilience in rapidly evolving technological environments compared to traditionally educated peers. Additionally, from corporate cybersecurity roles to government positions to entrepreneurial ventures, investigating how distributed agency competencies transfer across different professional contexts would provide crucial evidence for pedagogical effectiveness.

The development of specialized educational technologies designed for human-AI collaboration learning represents an opportunity for educational innovation. Rather than adapting existing AI tools for educational contexts, researchers should explore technologies that are purpose-built to facilitate assemblage learning, support collaborative sense-making processes, and enable assessment of distributed performance. This includes developing AI systems that can effectively participate in educational relationships while maintaining appropriate pedagogical boundaries and learning objectives.

Distributed agency concepts offer substantial potential for transformation in other fields where human-AI collaboration is becoming prevalent. Healthcare education, engineering programs, business analytics, and social work training all involve professional contexts where effective practice increasingly depends on human-AI collaboration. Adapting posthuman pedagogical principles developed for cybersecurity education could enhance professional preparation across multiple disciplines, creating opportunities for interdisciplinary pedagogical research.

As distributed agency pedagogy scales across institutions, research examining policy implications becomes crucial. This includes investigating how accreditation standards might adapt to recognize collaborative competencies, how academic integrity frameworks can evolve to support appropriate human-AI collaboration, and how institutional assessment policies might effectively measure distributed learning outcomes while maintaining educational quality standards.

### VIII. LIMITATIONS AND FUTURE RESEARCH

This framework development and preliminary implementation observations have limitations that constrain generalizability. The implementation context represents a single course at one institution with a specific student

population, limiting generalizability across diverse educational settings. The observations presented are preliminary and require systematic data collection, longitudinal tracking of student development, and comparative analysis across multiple implementations. Future empirical research should examine the framework's effectiveness through controlled studies measuring collaborative competency development, assessment validity in distributed agency contexts, and long-term professional outcomes for students educated through posthuman approaches. Additionally, research is needed on scalability factors, resource requirements, and institutional adaptation processes for broader adoption. The theoretical framework presented here serves as a foundation for such empirical investigation while providing immediate practical guidance for educators exploring posthuman approaches to cybersecurity education.

## IX. CONCLUSION

The integration of artificial intelligence into cybersecurity operations has created professional environments where effective security emerges from collaborative human-AI networks rather than individual expertise. This evolution demands cybersecurity education approaches that recognize and cultivate distributed agency across human-AI assemblages.

This analysis demonstrates how posthuman theoretical frameworks provide both conceptual foundation and practical guidance for distributed agency pedagogy in cybersecurity education. The preliminary implementation observations suggest that students can develop collaborative competencies when educational experiences are structured around assemblage principles rather than individual skill development, progressing from tool-based interactions toward integration of human-AI collaboration as a core professional competency through sustained relationship development.

For educators, implementing distributed agency pedagogy requires developing their own competencies in facilitating human-AI collaboration, creating assessment approaches evaluating assemblage performance, and orchestrating learning experiences where insights emerge from network interactions. Institutional support proves crucial for modifying assessment policies, academic integrity frameworks, and resource allocation to accommodate collaborative approaches.

The posthuman pedagogical principles demonstrated—designing for assemblages, cultivating relationality, embracing emergence, and developing distributed assessment approaches—offer frameworks for educational development across multiple disciplines where human-AI collaboration is becoming essential. As cybersecurity practice continues evolving toward more complex human-AI collaborative environments, distributed agency pedagogy offers theoretical foundation and practical strategies for preparing students to participate effectively in the posthuman assemblages increasingly characterizing contemporary practice.

## REFERENCES

- [1] R. Straight, "Decentering the Human: A Posthuman Approach to Cybersecurity Education," in *2024 Cyber Awareness and Research Symposium (CARS)*, Oct. 2024, pp. 1–6. doi: 10.1109/CARS61786.2024.10778862.
- [2] R. Braidotti, *The posthuman*. Cambridge: Polity Press, 2013.
- [3] B. Latour, *Reassembling the social: An introduction to actor-network-theory*. Oxford: Oxford University Press, 2005.
- [4] L. S. Vygotskij, *Mind in society: The development of higher psychological processes*. Cambridge, Massachusetts: Harvard University Press, 1978.
- [5] J. Lave and E. Wenger, *Situated Learning: Legitimate Peripheral Participation*. Cambridge: Cambridge University Press, 1991.
- [6] M. D. Merrill, "First principles of instruction," *Educational Technology Research and Development*, vol. 50, no. 3, pp. 43–59, 2002, doi: 10.1007/BF02505024.
- [7] R. M. Gagné, *The conditions of learning and theory of instruction*, 4th ed. New York: Holt, Rinehart; Winston, 1985.
- [8] D. A. Kolb, *Experiential learning: Experience as the source of learning and development*, 2nd ed. Upper Saddle River, NJ: Pearson Education, 2015.
- [9] H. S. Barrows, "Problem-based learning in medicine and beyond: A brief overview," *New Directions for Teaching and Learning*, vol. 1996, no. 68, pp. 3–12, 1996, doi: 10.1002/1l.37219966804.
- [10] C. Adams and T. L. Thompson, *Researching a Posthuman World*. London: Palgrave Macmillan UK, 2016. doi: 10.1057/978-1-137-57162-5.
- [11] D. Ihde, *Technology and the Lifeworld: From Garden to Earth*. Bloomington: Indiana University Press, 1990.
- [12] "Teaching as indwelling between two curriculum worlds: The coming into being of a Pedagogical Situation," in *Curriculum in a New Key: The Collected Works of Ted T. Aoki*, 1st ed., Routledge, 2004, pp. 159–165. Accessed: Sep. 18, 2025. [Online]. Available: <https://www.perlego.com/book/1554723/curriculum-in-a-new-key-the-collected-works-of-ted-t-aoki-pdf>
- [13] D. Belshaw, *The Essential Elements of Digital Literacies (v1.0)*, v1 ed. 2014. Accessed: Sep. 18, 2025. [Online]. Available: <https://dougbelshaw.com/essential-elements-book.pdf>
- [14] A. Gunder, J. Herron, N. Weber, C. Chelf, and S. Birdwell, "Opened Culture | Dimensions of AI Literacies," *Opened Culture*. 2024. Accessed: Sep. 18, 2025. [Online]. Available: <https://openedculture.org/projects/dimensions-of-ai-literacies/>
- [15] D. Haraway, *Staying with the trouble: Making kin in the Chthulucene*. Durham: Duke University Press, 2016.
- [16] N. Snaza et al., "Toward a posthumanist education," *Journal of Curriculum Theorizing*, vol. 30, no. 2, pp. 20–47, 2014.