Decentering the Human: A Posthuman Approach to Cybersecurity Education

Ryan Straight
Cyber, Intelligence, and Information Operations
University of Arizona
Tucson, AZ 85719
https://orcid.org/0000-0002-6251-5662

Abstract—**This brief paper introduces a paradigm shift in cybersecurity education, advocating for a move from human-centric models to a posthuman approach that acknowledges the distributed and interconnected nature of modern cyber ecosystems. By decentering human agency and recognizing the active role of non-human actors, particularly artificial intelligence (AI), the development of more comprehensive, adaptive, and resilient security strategies is possible. The paper explores the potential of posthuman approaches in addressing emerging threats in AI-driven environments and examines the implications for cybersecurity education. Through a critical analysis of current limitations in human-centric cybersecurity models and an exploration of key posthuman concepts, this research aims to contribute to the ongoing dialogue on the future of cybersecurity education in increasingly complex technological landscapes, offering a theoretical framework for integrating posthuman concepts into cybersecurity curricula and providing a foundation for future research and educational design.**

Keywords—posthumanism, human-centric, education, artificial intelligence, pedagogy

I. Introduction

As artificial intelligence and other emerging technologies dominate our digital landscape and lives, traditional human-centric approaches to cybersecurity education are becoming obsolete. While acknowledging the benefits of anthropocentricism, this paper proposes a paradigm shift towards a posthuman framework, one that acknowledges the distributed and interconnected nature of modern cyber ecosystems. By decentering human agency and recognizing the active role of non-human actors, particularly AI, we can develop more comprehensive, adaptive, and resilient security strategies and educational approaches, specifically in cybersecurity education.

By decentering, but not dismissing, human agency and recognition of the active role of non-human actors, particularly artificial intelligence (AI), the immense potential of posthuman approaches become apparent. This shift towards a posthuman approach to cybersecurity draws on theoretical frameworks that address the distributed nature of cognition and action across human-technological networks [1], [2]. Through examining current limitations in human-centric cybersecurity models and an exploration of key posthuman concepts, this research aims to contribute to the ongoing dialogue on the future of cybersecurity education in increasingly complex technological landscapes.

The aim here, then, is to explore the potential of posthuman approaches in cybersecurity practices and education, addressing emerging AI-driven environments, and navigating the implications of distributed agency in the cyber domain. By doing so, this brief paper seeks to make two key contributions to the field of cybersecurity education. First, it engages in critical analysis of the limitations of human-centric approaches in cybersecurity. Second, it offers a theoretical framework for integrating posthuman concepts into cybersecurity curricula, providing a foundation for future research and educational design.

II. A Humanist Cyber Domain

The field of cybersecurity has long been dominated by human-centric approaches, focusing primarily on user behavior, social engineering, and human-driven threat detection. This includes human rights, viewing communication networks as essential topics for study, advocating for global network integrity, strong encryption, and robust data protection measures [3]. This view–incorporating the human-centric view into cybersecurity education–is understood to better equip professionals to navigate the complex interplay between technological systems, ethical considerations, and human rights in our increasingly interconnected and digital world. This perspective places individuals and communities at the core of cybersecurity processes, emphasizing digital privacy, internet freedom, and the protection of digital human rights [4]. While states remain key actors in cybersecurity, a human-centered approach argues that security measures should not compromise individual rights and freedoms. This perspective is particularly relevant as cyber incidents increasingly impact human lives and well-being across various sectors. Integrating this human-centered view into cybersecurity education could contribute to better equipped professionals.

Recent research has highlighted the need to shift the perspective on human factors in cybersecurity from viewing humans solely as vulnerabilities to recognizing their potential as solutions. While human errors contribute significantly to cybersecurity incidents, organizations should focus on developing human-centric strategies to reduce these mistakes [5]. This approach involves implementing leadership-driven cybersecurity cultures, fostering organizational resilience, and leveraging human factors expertise to enhance security practices. By integrating these human-centric elements into cybersecurity education and training programs, organizations can create a more holistic and effective approach to addressing

© 2024 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
Accepted manuscript of: R. Straight, "Decentering the Human: A Posthuman Approach to Cybersecurity Education," in *2024 Cyber Awareness and Research Symposium (CARS)*, 2024, doi: 10.1109/CARS61786.2024.10778862. This is not the version of record.

cyber threats. This shift towards viewing humans as potential solutions rather than just problems in the cybersecurity chain aligns with the need for a more comprehensive, multifaceted approach to cybersecurity education.

Despite the critical role of human factors in cybersecurity, there is a notable absence of comprehensive human factors training in cybersecurity curricula [6]. This gap can instead leave future professionals ill-equipped to address the complex interplay between human behavior and technological systems. Organizations often mistakenly equate human factors issues with training problems, neglecting the broader psychological and cognitive aspects of cybersecurity [6]. To address this, cybersecurity education may broaden its scope and incorporate insights from human factors specialists, cognitive scientists, and behavioral analysts to develop more effective strategies for reducing human-enabled errors in information security.

Civil society organizations also play a vital role in promoting a human-centric approach to cybersecurity by positioning individuals as the primary beneficiaries of security measures. These groups contribute to cybersecurity efforts through capacity building, fostering transparency, and facilitating stakeholder dialogue [7]. Their involvement in areas such as vulnerability disclosure, incident response, and critical infrastructure policy helps balance technological solutions with ethical considerations and human rights. Incorporating civil society perspectives into cybersecurity education could thus enhance the field's ability to implement a more holistic, human-centered approach.

However, as our digital ecosystems become increasingly complex and interconnected, there is a growing need to reconsider this paradigm, particularly in the context of cybersecurity education. While the human-centric approach has made significant contributions to cybersecurity, it fails to fully capture the complex, interconnected nature of modern cyber environments. To further explore these limitations, a more targeted analysis of the anthropocentric perspective in cybersecurity education–prior to *post*-ing the humanism in the domain–is warranted.

III. Anthropocenric Cybersecurity Education

To effectively explore human-centric cybersecurity, education and training programs must consider individual characteristics such as gender, age, cultural background, and emotional responses. Research indicates that these factors can significantly influence cyber risk awareness and behavior [8], like gender differences in phishing awareness and cybercrime susceptibility, as well as age-related variations in self-efficacy and precautionary behaviors. Cultural background can affect password generation habits and overall cyber maturity levels across regions, and emotional responses to cyber threats vary based on individual identity and context. As such, this anthropocentric view has shaped the development of security measures and, consequently, cybersecurity education, but often fails to adequately capture the complex, interconnected nature of modern cyber environments. This limitation is particularly evident in the treatment of AI-driven threats and defenses, where machine learning systems can become both targets and vectors of attack [9]. The evolution of the cyber domain necessitates a new "onto-logic of action" to navigate its indeterminate and relationally protean nature [10].

While human factors play a crucial role in cybersecurity, there is a notable absence of comprehensive human factors training in cybersecurity curricula [11]. This gap leaves future professionals ill-equipped to address the complex interplay between human behavior and technological systems. The disconnect between conceptual knowledge and practical application of cybersecurity principles among young people further underscores the need for more effective educational approaches [12].

The gap between industry needs and academic preparation is also significant. Studies of cybersecurity programs at Centers of Academic Excellence in Cybersecurity (CAE-C) institutions reveal a disparity between industry-expected skill levels and those achieved by graduates [13]. This issue is compounded by the wide variation in cybersecurity course content across institutions and a lack of rigorous assessment methods [14]. Current research in cybersecurity education tends to focus on instructional tools and content rather than empirical evaluations of teaching efficacy, highlighting the need for more adaptive and theoretically grounded approaches [13], [14].

Beyond teaching and instructional materials, cultural context significantly influences cybersecurity awareness and behaviors, as well, challenging the efficacy of a one-size-fits-all approach to cybersecurity education [15]. Factors such as power distance, individualism-collectivism, risk perception, and trust in authorities shape cybersecurity attitudes and practices across different cultures. This cultural variability necessitates more nuanced, adaptable approaches to cybersecurity education that can address diverse social contexts.

No single approach or solution is perfect or foolproof, and this human-centric approach to cybersecurity education is no different. The limitations of these models extend beyond curriculum content to practical implementation, marked by inadequate teacher expertise, insufficient funding, and limited resources pose substantial challenges to effective cybersecurity education programs [16]. The pace of technological change often outstrips the adaptability of human-centered educational models, creating a mismatch between constantly evolving threats and educational responses.

To begin addressing these limitations, a posthuman perspective on cybersecurity education may offer valuable insights. This approach extends the recognition of agency to non-human actors in our digital environments [17]. By considering how AI systems–to use the most pressing and visible example in current discourse–contribute to both vulnerabilities and protections, we can develop more comprehensive and effective cybersecurity strategies that go beyond traditional, human-centered models. First, though, we must explore posthumanism and precisely what it is (and is not).

IV. Posthumanism in Its Many Forms

Posthumanism offers a reconceptualization of the relationships between humans, technology, and the environment. It challenges traditional anthropocentric worldviews and proposes a more inclusive understanding of agency and intelligence that extends beyond human boundaries.

This theoretical framework has emerged as a response to the limitations of humanist thinking and the increasing complexity of our technologically-mediated world.

At its core, posthumanism questions the foundational assumptions of classical humanism that have structured much of modern life and understanding [18]. It challenges the notion of 'Man' as the central figure of existence, distinct from animals, machines, and other nonhuman entities, and as the origin of meaning and history [19]. This critique extends to the liberal humanist idea of a universal human essence, which posthumanism argues is a construct rather than a natural given. It's crucial to note that posthumanism in this context refers to consideration beyond the human, rather than considering replacement of the human. The post in posthuman is analogous to its usage in postmodernism, signifying an expansion and critique of previous paradigms, not their obsolescence. As the present exploration moves deeper, this approach will point toward a broader understanding of agency, intelligence, and interaction in cybersecurity to include non-human actors, particularly AI systems, without diminishing the importance of human factors.

Posthumanist thought can be broadly categorized into three interrelated strands: critical, technological, and ecological posthumanism [18], and should not be conflated with transhumanism, which tends to focus on the extension of the human [20]. Critical posthumanism, however, rooted in poststructuralist and postcolonial theories, deconstructs the anthropocentric assumptions underlying traditional humanist philosophies. It argues that we are already posthuman, emphasizing how our existence is fundamentally shaped by our technological environment [1].

Technological posthumanism focuses on the ways in which human cognition and agency are extended through and intertwined with technological systems. This perspective challenges the idea of human exceptionalism by highlighting our increasing dependence on and integration with digital technologies[1]. It proposes that our cognitive processes extend beyond our brains to include external tools and technologies, blurring the boundaries between human and machine.

Ecological posthumanism emphasizes the interconnectedness of humans with their material and environmental ecologies[2]. This strand draws attention to the need for a post-anthropocentric worldview in the face of global ecological crises, arguing for a fundamental shift in how we conceive of humanity's place in the world and moving away from notions of human dominance over nature towards an understanding of humans as part of complex ecological systems.

These posthumanist perspectives share a common thread in their rejection of human exceptionalism and their emphasis on the distributed nature of agency across human and non-human actors. They challenge us to rethink fundamental concepts such as subjectivity, agency, and ethics in a world where the boundaries between human, animal, and machine are increasingly blurred. The implications are far-reaching, extending beyond academic discourse to influence how we understand and navigate our increasingly technologized world. By decentering the human subject and recognizing the agency of non-human actors, posthumanism provides a framework for addressing complex contemporary issues that transcend traditional disciplinary boundaries. This presents an intriguing and highly applicable method for analyzing the complex interplay between human users and technological systems in the cyber domain. It challenges us to move beyond notions of human-centered security and to consider the distributed and interconnected nature of agency in digital environments.

V. Posthuman Education, Cybersecurity, and Cybersecurity Education

Katherine Hayles, bringing the posthumanist notion of the cyborg to the forefront, describes the complex human/technology amalgam as having "no essential difference or absolute demarcation between bodily existence and computer simulation, cybernetic mechanism and biological organism, robot teleology and human goals" [1, p. 3]. Given the myriad ways in which professionals, consumers, and learners deeply engage with cyber-supported technologies, this blurring of boundaries supports the need to reevaluate our cybersecurity paradigms and how we educate future cybersecurity professionals.

Posthumanism offers several key concepts that can inform a new approach to cybersecurity education. The decentering of human agency challenges the notion that humans are the sole agents in complex systems, recognizing the agency of non-human actors, particularly AI systems. The concept of distributed cognition suggests that cognitive processes are not confined to individual human minds but are distributed across human-technological networks. Material-semiotic approaches, drawing from Actor-Network Theory [26], emphasize the importance of considering both human and non-human actors in understanding complex systems. These concepts provide a foundation for reimagining cybersecurity education in a way that acknowledges not only the active role of AI in both threat landscapes and defense strategies, but lays the groundwork for as-yet unimagined technologies.

A posthuman approach to cybersecurity education requires us to reconsider the role of human agency in cyber ecosystems[3]. At its core, "posthumanism asks us to attend to and take seriously that which is most near to us, the everyday things of our world" [25, p. 2]. In the context of cybersecurity education, this means recognizing that threats and vulnerabilities can emerge from the complex interactions between human and non-human actors, particularly AI systems, rather than solely from human intentions or actions. This shift in perspective allows us to consider how AI systems contribute to the security landscape in ways that may be overlooked by human-centric educational

[1] For further analysis of the extensive and expanding ways humans relate to technology and it mediates our existence, the empirical and non-essential approach of postphenomenology is key. See the works of Ihde [21], Rosenberger and Verbeek [22].

[2] The posthumanist framework and pedagogy discussed in this piece should be considered distinct from the environmentally driven analyses like those of Copeland et al. [23] or the ethopolitical arguments of Osborne and Rose [24], aligning instead with the posthuman inquiry approach of Adams and Thompson [25], for example.

[3] The irony of this work in the Human-Centric Cyber Security track is not lost on the author.

models. In complex cyber ecosystems, decision-making and threat response are often distributed across networks of human analysts, automated systems, and AI algorithms. Cybersecurity education should therefore prepare students to work effectively with and within these distributed cognitive systems, understanding how threat intelligence is gathered, processed, and acted upon by a combination of human analysts and AI systems. This approach aligns with the assertion that posthuman accounts should show evidence of attending to one's own "more-than-humanness" and explicitly engaging with non-human elements in the process [27].

Returning to Actor-Network Theory, a material-semiotic approach to cybersecurity education would consider both the technical and social aspects of cyber systems as part of a unified network. This perspective encourages students to trace the connections between various actors (human and non-human) in a cyber ecosystem, examining how they interact to produce security outcomes. For example, when analyzing a data breach, students should be taught to consider not just human errors or malicious actions, but also the complex interactions between user behaviors, AI-driven security systems, software vulnerabilities, and network configurations.

The rise of sophisticated AI systems presents new challenges for cybersecurity that go beyond traditional human-centric threat models. Cybersecurity education must adapt to prepare students for a landscape where AI systems can autonomously generate and execute cyber attacks, including understanding how AI can be used to create deepfakes and disinformation campaigns that operate at scales and with levels of sophistication beyond human capabilities. Students must also be equipped to address the challenges posed by automated hacking tools that can adapt and evolve their strategies in real-time, potentially outpacing human-driven defense mechanisms.

VI. Posthuman Implications for Cybersecurity Education and Artificial Intelligence

A posthuman perspective encourages us to consider how vulnerabilities can emerge from the complex interactions within AI-driven systems, often in ways that are difficult to predict or attribute to specific human actions. Cybersecurity education should therefore focus on developing students' abilities to analyze and understand these emergent phenomena. This includes examining how seemingly benign interactions between different AI components or algorithms can create unexpected security holes, and how the increasing complexity of AI systems can lead to emergent behaviors that create new attack surfaces.

Posthuman approaches also encourage us to consider how AI can play active roles in propagating cyber threats. Cybersecurity education should move beyond viewing AI systems as passive tools manipulated by human attackers, and instead recognize their potential for autonomous or semi-autonomous action. This includes studying how AI-driven botnets can self-propagate and evolve their attack strategies without direct human control, or how AI-enhanced malware can adapt its behavior to evade detection. By understanding these non-human actors as active agents in the threat landscape, students will be better prepared to develop effective countermeasures.

To be clear, this means adopting a posthuman approach to cybersecurity necessitates a fundamental shift in educational objectives. Rather than focusing solely on human-centric skills and knowledge, cybersecurity curricula should aim to develop students' abilities to understand, interact with, and leverage AI systems in security contexts. This includes fostering an understanding of AI's role as a potential threat, a powerful defensive tool, and a co-agent in the cybersecurity domain. Educational programs should emphasize the importance of viewing cybersecurity as a collaborative effort between human experts and AI systems, each with their own strengths and limitations.

Illustrative is a look at a typical approach to engaging in applied cybersecurity education: gamification through the "capture-the-flag" (CTF) model [28]. Viewing these experiences through a posthuman lens immediately raises a wide range of questions: how might the target audience change when considering non-human actors? How would the concepts or difficulty levels change when viewed through the posthuman framework? How might scoring, awarding, and statistics need to be reconsidered when non-human agents like AIs are involved? How would automatic and manual evaluation methods need to evolve? What new or different categories would need to be developed? Without careful attention paid to where, how, and why non-human agents are integrated, learners may actually find themselves at a disadvantage [29].

This approach would encourage students to think beyond classical logical principles and consider the multiple, sometimes contradictory, ontological formations that cyber threats and defenses can take. Cybersecurity education should prepare students to work effectively with varied AI-driven systems, which involves not only teaching the technical aspects of these systems but also developing students' ability to critically evaluate AI-generated insights and recommendations. Curricula should cover topics such as the development of AI systems that can autonomously detect, analyze, and respond to threats in real-time, as well as the potential for AI to identify patterns and anomalies that might be imperceptible to human analysts. Further, students must learn how to most effectively engage with these systems with respect to co-agency, considering the technical and ethical implications of delegating security decisions to AI systems.

Clearly, the complexity of AI-driven cyber environments requires an interdisciplinary approach to related education. Cybersecurity programs should incorporate elements of computer science, data science, ethics, and even cognitive psychology to provide students with a holistic understanding of the posthuman cyber landscape. This interdisciplinary focus will enable future cybersecurity professionals to navigate the complex interactions between human and non-human actors in cyber ecosystems more effectively.

VII. Ethical Considerations in Posthuman Cybersecurity Education

The posthuman approach to cybersecurity education therefore necessitates a reconceptualization of ethical frameworks to account for the distributed agency across human-AI networks and other technologies. Crucially, posthuman ethics requires us to think beyond anthropocentric notions of

moral responsibility and consider the ethical implications of our entanglements with non-human actors [2]. In the context of cybersecurity in general and cybersecurity education in particular, this means grappling with complex questions of responsibility, privacy, and decision-making in systems where agency is distributed between human and AI actors. Students must be prepared to navigate the implications of AI and machine learning for data privacy, particularly in terms of inference and data aggregation. This includes examining challenges to traditional notions of consent and data ownership in posthuman cyber ecosystems and exploring the potential for new forms of privacy-preserving technologies that align with posthuman principles.

As AI systems take on more active roles in cybersecurity, ensuring ethical decision-making becomes crucial. Cybersecurity education should incorporate frameworks for embedding ethical principles into AI security systems and address potential biases in AI decision-making processes. Students must learn to balance the need for instantaneous, highly complex, automated responses with ethical considerations and appropriate human oversight

VIII. Conclusion

This brief paper has argued for a fundamental theoretical shift in cybersecurity education, moving from human-centric models to a posthuman approach that recognizes the distributed, interconnected nature of modern cyber ecosystems. By decentering human agency and acknowledging the active role of AI as non-human actors, we can develop more comprehensive, adaptive, and resilient security strategies and educational approaches.

The posthuman perspective offers valuable insights into emerging threats, from AI-generated attacks to vulnerabilities arising from complex system interactions. It also points the way toward innovative educational strategies that prepare future cybersecurity professionals to work effectively in AI-driven environments. These strategies include the reframing of educational objectives to emphasize collaborative human-AI approaches to cybersecurity, integrating AI-driven defense strategies into curricula, including critical evaluation of AI-generated insights, and fostering interdisciplinary approaches that combine technical knowledge with ethical considerations and cognitive understanding. However, this shift also raises significant ethical questions about responsibility, accountability, and the nature of decision-making in cybersecurity contexts. Likewise, implementing these changes may face resistance from traditional educational structures and require significant resource allocation for curriculum development and faculty training. As we move forward, it will be crucial to navigate these challenges thoughtfully, balancing the potential benefits of posthuman approaches with careful consideration of their broader implications.

Ultimately, embracing a posthuman paradigm in cybersecurity education is not just about adopting new technologies or strategies. Instead, it represents a fundamental reconsideration of our relationship with AI, especially, and other non-human actors in digital systems, challenging us to think beyond traditional boundaries and imagine new possibilities contemporary and looming security across domains. Future research should focus on developing concrete pedagogical approaches and curricula that embody these posthuman principles, as well as empirical studies to assess their effectiveness in preparing cybersecurity professionals for the challenges of AI-driven environments.

References

[1] N. K. Hayles, How we became posthuman: Virtual bodies in cybernetics, literature, and informatics. The University of Chicago Press, 1999 [Online]. Available: https://hdl.handle.net/2027/heb05711.0001.001

[2] F. Ferrando and R. Braidotti, Philosophical Posthumanism. London, UNITED KINGDOM: Bloomsbury Publishing Plc, 2019 [Online]. Available: http://ebookcentral.proquest.com/lib/uaz/detail.action?docID=5790558

[3] R. J. Deibert, "Toward a Human-Centric Approach to Cybersecurity," Ethics & International Affairs, vol. 32, no. 4, pp. 411–424, Dec. 2018.

[4] C. M. Codreanu, "Exploring the Need for Human-Centred Cybersecurity. The Wannacry Cyberattack." Rochester, NY, Dec-2021.

[5] N. C. Edeh, "Cybersecurity and Human Factors: A Literature Review," in Cybersecurity for Decision Makers, CRC Press, 2023.

[6] C. Nobles, "Botching Human Factors in Cybersecurity in Business Organizations," HOLISTICA – Journal of Business and Public Administration, vol. 9, no. 3, pp. 71–88, Nov. 2018.

[7] S. Kumar, "The Missing Piece in Human-Centric Approaches to Cybernorms Implementation: The Role of Civil Society," Journal of Cyber Policy, vol. 6, no. 3, pp. 375–393, Sep. 2021.

[8] K. Jadhav, S. Haggag, and H. Haggag, "Diving deep into human centric issues within cyber security," in Joint 4th International Workshop on Experience with SQuaRE Series and Its Future Direction and 1st Asia-Pacific Software Engineering and Diversity, Equity, and Inclusion Workshop, IWESQ 2022 + APSEDEI 2022, 2022, pp. 60–68.

[9] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," Pattern Recognition, vol. 84, pp. 317–331, Dec. 2018.

[10] S. L. Pratt and J. L. Rosiek, "The Logic of Posthuman Inquiry: Affirmative Politics, Validity, and Futurities," Qualitative Inquiry, p. 10778004231162075, May 2023.

[11] C. Nobles, N. Robinson, M. Cunningham, N. Robinson, M. Cunningham, and M. Cunningham, "Straight From the Human Factors Professionals' Mouth: The Need to Teach Human Factors in Cybersecurity," in Proceedings of the 23rd Annual Conference on Information Technology Education, 2022, pp. 157–158.

[12] J. Nicholson, J. Terry, H. Beckett, and P. Kumar, "Understanding Young People's Experiences of Cybersecurity," in Proceedings of the 2021 European Symposium on Usable Security, 2021, pp. 200–210.

[13] J. Crabb, C. Hundhausen, and A. Gebremedhin, "A Critical Review of Cybersecurity Education in the United States," in Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1, 2024, pp. 241–247.

[14] V. Švábenský, J. Vykopal, and P. Čeleda, "What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences," in Proceedings of the 51st ACM Technical Symposium on Computer Science Education, 2020, pp. 2–8.

[15] M. U. Shah, F. Iqbal, U. Rehman, and P. C. K. Hung, "A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance," IEEE Access, vol. 11, pp. 87970–87984, 2023.

[16] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The Importance of Cybersecurity Education in School," International Journal of Information and Education Technology, vol. 10, no. 5, pp. 378–382, 2020.

[17] J. Ulmer, "Posthumanism as Research Methodology: Inquiry in the Anthropocene," International Journal of Qualitative Studies in Education, vol. 30, pp. 832–848, Oct. 2017.

[18] S. Bayne, "Posthumanism: A Navigation Aid for Educators," On Education. Journal for Research and Debate, vol. 1, no. 2, Sep. 2018.

[19] R. Braidotti and M. Hlavajova, Eds., Posthuman Glossary. London: Bloomsbury Publishing Plc, 2018.

[20] A. C. Porter, "Transhumanism and Posthumanism(s) on Education," International Journal of Philosophical Studies, vol. 31, no. 4, pp. 475–500, Aug. 2023.

[21] D. Ihde, "Introduction: Postphenomenological research," Human Studies, vol. 31, no. 1, pp. 1–9, 2008.

[22] R. Rosenberger and P.-P. Verbeek, "A Field Guide to Postphenomenology," in Postphenomenological Investigations: Essays on Human-Technology Relations, Lexington Books, 2015, pp. 9–41.

[23] K. Copeland et al., "Posthuman pedagogy: Experiential education for an era of mutualism," Environmental Education Research, vol. 29, no. 10, pp. 1443–1459, Oct. 2023.

[24] T. Osborne and N. Rose, "Against Posthumanism: Notes towards an Ethopolitics of Personhood," Theory, Culture & Society, vol. 41, no. 1, pp. 3–21, Jan. 2024.

[25] C. Adams and T. L. Thompson, Researching a Posthuman World. London: Palgrave Macmillan UK, 2016.

[26] Bruno. Latour, Reassembling the Social: An Introduction to Actor-Network-Theory. Oxford, UNITED KINGDOM: Oxford University Press, Incorporated, 2005 [Online]. Available: http://ebookcentral.proquest.com/lib/uaz/detail.action?docID=422646

[27] T. L. Thompson and C. Adams, "Accountabilities of posthuman research," Explorations in Media Ecology, vol. 19, no. 3, pp. 337–349, Sep. 2020.

[28] A. Rehaimi, Y. Sadqi, and Y. Maleh, "A Comparative Study of Online Cybersecurity Training Platforms," in Verification and Evaluation of Computer and Communication Systems, 2024, pp. 122–134.

[29] W. Tann, Y. Liu, J. H. Sim, C. M. Seah, and E.-C. Chang, "Using Large Language Models for Cybersecurity Capture-The-Flag Challenges and Certification Questions." arXiv, Aug-2023 [Online]. Available: https://arxiv.org/abs/2308.10443