CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 4, No. 1
April 2025
ISSN: 2832-1006

In this issue:

4. Education Impact on Trust in Election Technology & Security: Research Proposal
Garry White, Texas State University
Ju Long, Texas State University

13. Cybersecurity Apprenticeships: Case-Study of a Four-Year Youth Apprenticeship Program
Paul Wagner, University of Arizona
Cathleen Barton, Cathleen Barton Consulting

24. *Teaching Case*
Reshaping Cybersecurity Ethics Education: Evaluating a Posthumanist Pedagogy Using Human/AI Co-Generated Case Studies
Ryan Straight, University of Arizona
Jonathan Lowery, University of Arizona
David Poehlman, University of Arizona
Waamene Yowika, University of Arizona

35. A Pivotal Progression of SEC's Cybersecurity Disclosure Requirements
Yining Chen, Western Kentucky University
Divine Lokuku, Western Kentucky University
Tong Wu, Western Kentucky University

©2025 ISCAP (Information Systems and Computing Academic Professionals)

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2025 ISCAP Board of Directors

Amy Connolly James Madison University President	Michael Smith Georgia Institute of Technology Vice President	Jeff Cummings Univ of NC Wilmington Past President
David Firth University of Montana Director	Mark Frydenberg Bentley University Director/Secretary	David Gomillion Texas A&M University Director
Leigh Mutchler James Madison University Director	RJ Podeschi Millikin University Director/Treasurer	Jeffry Babb West Texas A&M University Director/Curricular Matters
Eric Breimer Siena College Director/2024 Conf Chair	Tom Janicki Univ of NC Wilmington Director/Meeting Planner	Xihui "Paul" Zhang University of North Alabama Director/JISE Editor

Copyright ©2025 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to editorcppj@iscap.us.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

Anthony Serapiglia
Co-Editor
Saint Vincent College

Jeffrey Cummings
Co-Editor
University of North Carolina Wilmington

Thomas Janicki
Publisher
University of North Carolina Wilmington

2025 Review Board

Cheryl Beauchamp
Regent University

Ulku Clark
Univ of NC Wilmington

Peter Draus
Robert Morris University

Nick Giacobe
Penn State University

Mike Hills
Penn State University

Jeff Landry
Univ of South Alabama

Li-Jen Lester
Sam Houston State Univ

Jim Marquardson
Robert Morris University

Stan Mierzwa
Kean University

Etezady Nooredin
University of New Mexico

Ron Pike
Cal Poly Pomona

RJ Podeschi
Milliken University

Samuel Sambasivam
Woodbury University

Kevin Slonka
Saint Francis University

Geoff Stoker
Univ of NC Wilmington

Paul Wagner
University of Arizona

Ping Wang
Robert Morris University

Tobi West
Coastline College

Johnathan Yerby
Mercer University

Teaching Case:

Reshaping Cybersecurity Ethics Education: Evaluating a Posthumanist Pedagogy Using Human/AI Co-Generated Case Studies

Ryan Straight
ryanstraight@arizona.edu

Jonathon Lowery
jrl84623@arizona.edu

David Poehlman
dpoehlman@arizona.edu

Waamene Yowika
waamene@arizona.edu

Cyber, Intelligence, and Information Operations Department
University of Arizona
Tucson, AZ 85719

Hook

As the lines between human intuition and machine intelligence blur, AI-powered case studies push the boundaries of how we design and deliver instructional materials, offering a glimpse into the future of cyber praxis.

Abstract

This paper investigates the development, implementation, and pedagogical efficacy of AI-generated case studies and scenarios for cybersecurity ethics education. Employing a generative AI model, we developed learning materials for a cybersecurity ethics course, emphasizing a collaborative human-AI approach that resulted in a series of realistic and complex scenarios. These scenarios address core ethical concepts, foster critical thinking, and demonstrate adaptability to diverse learning preferences while maintaining relevance to contemporary cybersecurity challenges. While challenges such as advanced terminology use were identified through qualitative feedback, they were addressed through targeted interventions. This work situates itself within a posthumanist inquiry framework, exploring the evolving, co-constitutive relationship between human and non-human entities in educational contexts. Findings from a pilot implementation (n=23) indicate that the AI-generated scenarios significantly enhanced student engagement and perceived learning outcomes, with over 90% of participants reporting improved comprehension of core concepts and critical thinking proficiencies. This study contributes to the discourse on the intersection of AI, cybersecurity, and education, highlighting the potential of posthumanist pedagogical approaches.

Keywords: case studies, scenarios, artificial intelligence, posthumanism, ethics, teaching

Recommended Citation: Straight, R., Lowery, J., Poehlman, D., Yowika, W., (2025). Reshaping Cybersecurity Ethics Education: Evaluating a Posthumanist Pedagogy Using Human/AI Co-Generated Case Studies. *Cybersecurity Pedagogy and Practice Journal.* v4, n1, pp 24-34. DOI#: https://doi.org/10.62273/DTJD9647

©2025 ISCAP (Information Systems and Computing Academic Professionals)

Reshaping Cybersecurity Ethics Education: Evaluating a Posthumanist Pedagogy Using Human/AI Co-Generated Case Studies

Ryan Straight, Jonathan Lowery, David Poehlman and Waamene Yowika

1. INTRODUCTION

The integration of artificial intelligence (AI) into cybersecurity practices has propelled ethical considerations to the forefront, transforming them from mere discussion points into fundamental challenges to traditional notions of human agency, particularly within educational contexts. As cybersecurity professionals increasingly encounter complex ethical dilemmas with the potential to shape societal and cultural trajectories, the role of ethical principles in guiding the responsible development and implementation of AI systems becomes paramount (Blanken-Webb et al., 2018; González et al., 2024). This is particularly crucial given the significant global shortage of qualified cybersecurity professionals, estimated at 3.4 million in 2022 (Lake, 2022). This workforce deficit, coupled with the heightened demand for cybersecurity expertise, has intensified the focus on cybersecurity education (Matei & Bertino, 2023; P. Wang, 2022). The situation is further complicated by the fact that cybersecurity specialists often confront unpredictable ethical dilemmas that are not adequately addressed by existing legal frameworks or codified standards (Adaryukova et al., 2020). This lack of definitive guidelines, combined with the emerging potential of human-AI collaboration in educational content creation, underscores the imperative for innovative pedagogical approaches in cyber ethics education. These approaches must not only address the technical skills gap but also foster a nuanced understanding of the ethical complexities inherent in the cybersecurity domain.

A logical starting point for comprehending this evolving pedagogical landscape is to examine the established learning benchmarks and standards. The K-12 Cybersecurity Learning Standards, developed by CYBER.ORG (Cyber Innovation Center & CYBER.ORG, 2021), provide a comprehensive framework for introducing students to foundational cybersecurity concepts and equipping them with the requisite technical skills and knowledge to pursue careers in the field. Likewise, the National K12 Cybersecurity Education Roadmap (National Initiative for Cybersecurity Education (NICE), 2021) maintains a coordinated portfolio of national K12 cybersecurity education activities, designed to ensure the effective deployment of resources and optimize impact. At the post-secondary level, the National Security Agency's (NSA) Centers of Academic Excellence designations provide guidance aimed at establishing "standards for cybersecurity curriculum and academic excellence" (ibid.). Collectively, these initiatives, alongside the NSA's 2024 development of AI-focused standards, underscore the fundamental integration of AI across all cyber-related domains, particularly within education, signaling a shift towards even more technology-integrated learning environments.

However, translating theoretical AI ethics principles into practical pedagogical applications remains a significant challenge. The gap in formal ethical training and clearly defined ethical criteria for educating future cybersecurity experts (Jackson et al., 2023) has created an opening for the development of cognitive assemblages (Hayles, 1999)—synergistic interactions between human and artificial intelligence—in educational contexts. This paper posits that a posthumanist theoretical framework offers a valuable lens through which to examine this pedagogical innovation and the evolving, co-constitutive relationship between humans and AI in educational settings. One promising approach is the use of AI-generated case studies and scenarios, which can provide students with dynamic and engaging learning experiences while simultaneously instantiating intra-action (Barad, 2007) between human learners and technologically-mediated scenarios. This framework conceptualizes the learner and learning material not as pre-existing, independent entities, but rather as mutually constituted through their interaction, highlighting the dynamic interplay between human cognition and AI-generated content.

This paper investigates the development, implementation, and pedagogical efficacy of AI-generated case studies and scenarios for teaching cyber ethics, law, and policy, considering three crucial contexts: the current state of cybersecurity education, the imperative for diverse and inclusive approaches, and the

©2025 ISCAP (Information Systems and Computing Academic Professionals)

implications of AI for pedagogy. Grounded in both posthumanist theoretical frameworks and empirical evidence derived from a pilot implementation (n=23), we analyze how the collaborative interplay between human and artificial intelligence can yield effective learning materials while simultaneously challenging traditional notions of agency and expertise in educational contexts. This investigation contributes to the broader scholarly discourse on the intersection of AI, cybersecurity, and education, highlighting both the practical efficacy and theoretical implications of innovative posthuman pedagogical approaches, particularly the potential for AI-generated scenarios to foster deep engagement and enhance learning outcomes in cybersecurity ethics education.

2. LITERATURE REVIEW

A robust cybersecurity education should adopt a holistic approach, integrating both technical and non-technical content, and be grounded in rigorous research (Austin, 2020; Blair et al., 2020). The integration of ethics within the cyber domain is particularly crucial yet complex, requiring a nuanced balance between competing interests, such as security and civil rights. Moreover, accelerating technological advancement necessitates a continuous reevaluation of ethical considerations, which often serve as a catalyst for policy development (Navdeep, 2022). Existing pedagogical approaches in cyber education have increasingly incorporated ethics into cybersecurity curricula, aiming to cultivate students' ethical awareness and decision-making skills (Adaryukova et al., 2020; P. Wang, 2022). These initiatives underscore the growing recognition of the importance of such integration. However, mere memorization of laws and codes of ethics does not constitute a comprehensive ethics education for cybersecurity, a field that remains under-studied and insufficiently addressed in academic discourse (Blanken-Webb et al., 2018; Dexter et al., 2013). To tackle these limitations, innovative pedagogical approaches that actively engage students in realistic ethical decision-making scenarios are imperative.

Scenario- and case study-based pedagogical approaches have proven effective in introducing major domain concepts in technical cyber skills training, such as penetration testing (X. Wang & Bai, 2022). Furthermore, their efficacy has been demonstrated in the domain of cyber ethics education, providing students with practical experience in analyzing ethical dilemmas, immersing them in realistic scenarios, and fostering ethical reasoning skills (Adaryukova et al., 2020; Blanken-Webb et al., 2018). Similarly, interactive and game-based learning have been identified as effective methods for increasing awareness and interest in cybersecurity and related career paths (Triplett, 2023). However, curricular constraints, such as time limitations and a scarcity of readily available resources, can impede the implementation of these approaches (Kilhoffer et al., 2023). Moreover, early and structured ethical training related to AI applications in cybersecurity is necessary to bridge the gap between students' perceived and actual ethical preparedness (Matei & Bertino, 2023).

In addition to the pedagogical challenges, the field of cybersecurity education faces significant hurdles in terms of diversity and inclusion. Notably, women remain underrepresented in the cybersecurity workforce (Pinchot et al., 2020), necessitating the implementation of novel recruitment strategies targeting females across the K-20 educational spectrum (Rowland et al., 2018). Research indicates that girls often demonstrate improved learning outcomes when pedagogical approaches incorporate socialization and frequent interaction (Kim, 2016). Furthermore, peer mentorship has been identified as a critical factor in the success of cybersecurity programs for both women and men (Pinchot et al., 2020).

The integration of AI into educational practices raises fundamental questions about the nature of learning and the role of technology in shaping educational experiences. While much of the extant literature on AI in education conceptualizes AI as a tool subservient to teaching and learning (Veletsianos et al., 2024), this perspective may not fully encompass the complex relational interactions already underway between humans and AI (Woodward, 2023). As AI systems continue to advance, the potential for them to develop consciousness or sentience cannot be *entirely* dismissed, raising ethical considerations about the possibility of granting them certain protections and responsibilities typically associated with personhood (Osborne & Rose, 2024). However, it is crucial to acknowledge that current AI systems still–at time of publication–exhibit significant limitations when compared to human capabilities, and companies like Google strongly refute assertions that their advanced language models have attained any form of sentience (ibid.). The future role of AI as virtual and persistent, lifelong pedagogical agents remains uncertain yet plausible, thereby necessitating a continuous and consistent

reevaluation of educational approaches involving AI.

The successful integration of AI into educational practices is also contingent upon teachers' perceptions of educational technology and their willingness to adapt traditional pedagogical methods (Lin, 2022). Furthermore, students require adequate training and time to effectively utilize AI-assisted learning tools. AI-powered text analysis tools can be effectively integrated into innovative pedagogical approaches (O'Halloran, 2020), and story completion methods can be employed to elicit deeper insights from participants while fostering agency and creativity (Veletsianos et al., 2024).

As education confronts a period of rapidly accelerating change, it is imperative to consider novel approaches to thinking and teaching (Wallin, 2017). By affording students realistic and engaging learning experiences, AI-generated case studies and scenarios can contribute to the development of the ethical awareness and decision-making skills necessary for navigating the complex ethical dilemmas they are likely to encounter as future cybersecurity professionals (Adaryukova et al., 2020; Blanken-Webb et al., 2018).

3. METHODOLOGY

The study employed a developmental research approach within the context of a Cyber Ethics course. The course aligns with the National Security Agency's (NSA) required knowledge units for a Center of Academic Excellence in Cyber Operations (CAE-CO), and the learning objectives for each module are meticulously aligned with these requirements. To develop engaging and intellectually stimulating scenarios for the course's seven modules, an iterative, AI-assisted scenario development process was used. This process leveraged the capabilities of the Claude 3 Opus model, a generative AI developed by Anthropic PBC. The AI model was provided with comprehensive guidelines including the learning objectives, key concepts, readings, lecture notes, and desired complexity level for each module. A team of collaborators, consisting of one graduate student (JL) previously enrolled in the graduate version of the course and two undergraduate students (WY and DP), played an integral role in providing feedback and guidance throughout the development process. The AI model generated an initial set of scenarios based on the provided guidelines, which were subsequently reviewed and refined based on collaborator feedback. This feedback focused on assessing the relevance, clarity, level of engagement, and alignment of the scenarios with the specified learning objectives. This iterative process continued until a final set of scenarios was developed, representing a co-constitutive entanglement between human and artificial intelligence, as conceptualized within a posthumanist framework.
.

4. SCENARIO DEVELOPMENT

The AI-assisted scenario development process made possible the rapid and efficient creation of multiple scenarios tailored to the specific pedagogical needs of the course and informed by the perspectives of current and prospective students. This approach aimed to ensure that the scenarios were engaging, relevant, and effective in promoting critical thinking and fostering meaningful discussions surrounding the ethical, legal, and policy considerations inherent in the cyber domain. Scenarios were developed for each of the seven modules in the course. Each module addresses a distinct aspect of the subject matter, aligned with the NSA's CAE-CO knowledge unit requirements:

- **Module 1**: Examination of the evolution from classical Western ethical thought to cyber ethics, exploring how traditional moral frameworks adapt to digital environments, and establishing foundational concepts in information ethics.
- **Module 2**: Introduction to the fundamental concepts of cybersecurity ethics, including ethical frameworks and principles that guide decision-making processes in this domain and the contemporary philosophical underpinnings thereof.
- **Module 3**: Examination of the legal landscape governing cybersecurity, exploring relevant laws, regulations, and judicial precedents.
- **Module 4**: Focus on the policy dimensions of cybersecurity, discussing the roles and responsibilities of various stakeholders—including governments, organizations, and individuals—in shaping cybersecurity policies.
- **Module 5**: Addressing the ethical and legal implications of privacy and data protection within the context of cybersecurity, a particularly critical topic in the contemporary digital age.
- **Module 6**: Examination of the ethical and legal considerations surrounding cybercrime and cybersecurity incidents,

including issues such as attribution, jurisdiction, and response mechanisms.
- **Module 7**: Exploration of the future trajectory of cybersecurity ethics, law, and policy, considering the potential impact of emerging technologies and the evolving threat landscape.

The AI generated scenarios designed to be realistic and relevant to contemporary cybersecurity challenges. This was accomplished using the Quarto scientific publishing system to create interactive, rich documents, while using plain text markdown and CSS for styling. As such, they maintained readability and portability when engaging with the AI model. Module 5, for example, featured a scenario exploring the legal and ethical ramifications of a fictional smart home device company surreptitiously collecting and sharing user data. The final scenarios emulated a dossier-like format, incorporating an overview, diverse background information, "main characters" who served as individuals of interest, and a detailed timeline. To increase realism, each case included fabricated supplementary materials described above. This format not only provided students with a realistic perspective but also allowed for the integration of other relevant cyber-related skills, such as open-source intelligence gathering through detailed readings, while necessitating deep, critical engagement with the materials.

5. TEACHING GUIDE

Notwithstanding the relative ease and expediency afforded by contemporary generative AI, the effective integration of AI-generated scenarios into the curriculum necessitates meticulous planning and skilled facilitation to ensure that students engage in meaningful discussions and cultivate a profound understanding of the domain. In conjunction with the provided supplemental materials, the following teaching guide outlines the process for incorporating the scenarios into the course, encompassing suggested discussion questions, activities, and strategies for fostering productive conversations.

1. Introduction and Contextualization: begin by contextualizing each scenario within the framework of the corresponding module's learning objectives. This approach enables students to concretely identify the relevance of the scenario and discern the key concepts upon which they should focus. Subsequently, provide a succinct overview of the scenario, introducing its principal characters or stakeholders to establish a foundation for the ensuing discussion.
2. Engaging with the Scenario: encourage active engagement with the scenario through carefully crafted discussion questions and interactive activities.
    - Discussion Questions: discussion questions constitute a critical component of the teaching guide, as they prompt students to engage in critical thinking about the scenario and explore its multifaceted ethical, legal, and policy dimensions. For each scenario, develop a set of open-ended questions that encourage students to consider the perspectives of diverse stakeholders, analyze the potential ramifications of various courses of action, and evaluate the scenario through the lens of pertinent ethical frameworks and legal principles.
    - Interactive Activities: in addition to discussion questions, incorporate activities that enable students to actively engage with the scenario and apply their knowledge in a practical manner. For instance, students could be tasked with role-playing different stakeholders in the scenario, debating the merits of various courses of action, or presenting arguments for or against a particular decision. Alternatively, students could collaborate in small groups to formulate guidelines or recommendations for addressing the ethical, legal, or policy challenges presented in the scenario.
3. Facilitating Meaningful Discussions: when facilitating discussions, draw explicit connections between the scenarios and real-world events or current developments in the cybersecurity domain. This approach helps students apprehend the relevance and applicability of the concepts they are learning to authentic contexts. Encourage students to share their personal experiences or insights related to the scenario to further enrich the discussion and promote peer-to-peer learning. A posthumanist-informed pedagogy encourages explicit consideration of the AI's role in shaping the scenarios and the attendant ethical

complexities. This pedagogical approach invites students to critically examine the co-constitutive nature of human-AI interaction in the context of scenario development.

4. Cultivating a Safe and Inclusive Environment: to facilitate meaningful and productive discussions, it is imperative to cultivate a safe and inclusive learning environment where all students feel empowered to articulate their thoughts and perspectives. Establishing ground rules for respectful dialogue and encouraging active listening are essential to fostering a constructive exchange of ideas. As the instructor, guide the discussion, elucidate concepts when necessary, and ensure that all students have the opportunity to contribute.
5. Extending Learning Beyond the Classroom: conclude by providing students with resources for further learning and exploration, such as supplementary readings, case studies, or online resources that delve deeper into the ethical, legal, and policy aspects of cybersecurity. Encourage students to continue engaging with these topics beyond the classroom to foster a more comprehensive understanding of the field and better prepare them for future challenges in their professional endeavors.

The development and utilization of fictional—which is to say realistic but not verifiably real—case studies and scenarios has been demonstrated to be effective for fostering engagement and eliciting varied student responses (Orchard, 2019). To illustrate the potential impact and pedagogical affordances of such AI-generated scenarios, the student co-authors of this work—who also assisted in the development of scenarios—provide the following perspective in a later section.

6. STUDENT PERSPECTIVES

AI-generated scenarios offer numerous benefits for engaging students in the study of cyber ethics, law, and policy. By leveraging accurate information from pre-verified sources and real-life similarities, AI models can craft lifelike scenarios that captivate students' attention and provide them with realistic contexts to explore complex concepts. The depth and breadth of the content presented in these scenarios can keep students engaged and motivated to learn more about the subject matter, sparking interest in further self-study. One of the key advantages of AI-generated scenarios is their adaptability to different learning preferences in terms of modality, presentation, and interaction. These scenarios can be tailored to address contemporary issues related to cyber ethics and legislation, making the content more relevant and engaging for students.

In addition to the benefits mentioned above, AI-crafted scenarios can be created in a fraction of the time compared to traditional methods. AI models can utilize accurate information previously ingested by programmers and maintainers to craft scenarios, such as through the use of locally stored, pre-verified material or corroborated web-based content. Furthermore, these scenarios can be cross-referenced with other up-to-date models and real-life similarities using prompting techniques, thereby adding depth and value that can captivate students.

However, it is important to acknowledge the challenges associated with AI-generated scenarios. While models like ChatGPT can create compelling and easily digestible content, they may occasionally utilize terminology that is beyond the understanding of students new to the material. To mitigate this issue, providing a list of necessary terminology definitions can help ensure that students are well-informed and equipped to engage with the scenarios effectively.

The use of AI-generated scenarios in learning can be likened to the "Method, Opportunity, and Motive" model in cybersecurity. In this context, the AI-crafted scenarios serve as the method, providing students with the opportunity to explore and learn from realistic situations. While the initial motive may be to achieve a passing grade, the ultimate goal is to foster a genuine interest in the subject matter, encouraging students to pursue further learning independently.

Taken altogether, such AI-generated scenarios offer a powerful tool for engaging students in the study of cyber ethics, law, and policy. By providing realistic, adaptable, and thought-provoking content, these scenarios can captivate students' interest, promote practical application of complex concepts, and contribute to a more effective and engaging learning experience.

7. PILOT IMPLEMENTATION AND ANALYSIS

To evaluate the pedagogical efficacy of these AI-generated scenarios, a pilot implementation was conducted, followed by a comprehensive

quantitative and qualitative analysis, the findings of which are presented in the following section. The assessment protocol, theoretically grounded in posthumanist principles, used 5-point Likert-scale items and open-ended questionnaires to assess participant engagement, perceived learning gains, and the perceived efficacy of the scenarios in addressing topics within the domains of ethics, law, and policy. The protocol was specifically designed to capture traditional pedagogical metrics, identify indicators of intra-action between participants and the AI-generated content, and to acknowledged the "cognitive assemblage" (Hayles, 1999)–the synergistic interaction between human learners and AI-generated content–seeking to understand how this relationship manifests in educational outcomes. Data collection was conducted during the fall semester, engaging all enrolled students in the course. The response rate was 100% (n=25), with one response being incomplete, and one response being an outlier, and thus removed from quantitative analysis. The assessment instrument was designed to capture both traditional pedagogical metrics and indicators of intra-action between human learners and the technologically-mediated scenarios.

It is important to acknowledge the limitations of self-reported data, however. To mitigate, survey responses were unidentified, triangulated between quantitative (Likert) and qualitative (open-ended questions) data, allowing for cross-referenced validation, and participants were not provided any compensation or accolades. Despite these precautions, it's understood that self-reported perceptions may not perfectly correlate with improvements in domain mastery. This limitation presents opportunities for future research that is currently being designed.

8. RESULTS

Analysis of the survey data revealed compelling evidence for the effectiveness of AI-generated scenarios in fostering student engagement and facilitating deep learning in cyber ethics education. The quantitative data indicated consistently positive responses across three key dimensions: engagement with the AI-generated materials, perceived learning outcomes, and scenario effectiveness (see Table 1).

Table 1: Percentage of students who agreed or strongly agreed with statements about the AI-generated case studies.

Statement	M	SD	% Agree
The scenarios captured my interest.	4.65	0.49	100.0
The scenarios helped me understand key course concepts.	4.26	0.81	91.3
The scenarios were more engaging than traditional lectures.	4.35	0.71	95.7
The scenarios motivated me to think deeply about the issues.	4.30	0.70	95.7
The scenarios increased my confidence in applying course concepts.	4.17	0.78	91.3
The scenarios helped me grasp the complexities of the subject matter.	4.17	0.78	91.3

Note. Agreement reflects the percentage of students who selected "Agree" or "Strongly Agree" on a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree).

.

The scenarios proved particularly effective in conveying complex ethical concepts. Students reported high levels of engagement with the material, with the majority indicating strong agreement that the scenarios motivated deeper thinking about cyber ethics, law, and policy issues. This engagement demonstrably translated into perceived learning outcomes, with students reporting an improved understanding of key concepts (M = 4.26, SD = 0.81) and increased confidence in applying course content to real-world situations (M = 4.17, SD = 0.78). This suggests the formation of *posthuman ethical assemblages* or learning environments where ethical understandings emerge not from solely directed interactions of humans *at* content, but rather a dynamic interaction between learners, the case studies, and the AI-based technical infrastructure that facilitates their interaction.

Thematic analysis of qualitative responses identified several recurring patterns that point to the posthuman dimensions of the AI-generated scenarios. Students consistently emphasized the value of multiple document types (news stories, social media posts, leaked emails, law enforcement reports, so on) and perspectives in enhancing their understanding of complex cybersecurity situations. As one participant articulated, "the integration of the AI Avatar into daily life was particularly fascinating and made the ethical implications feel more immediate and relevant." This finding aligns with "transversal connections" (Ferrando & Braidotti, 2019),

underscoring the participants' intuitive linking of the scenarios' technical dimensions to broader socio-ethical considerations.

Analysis of scenario effectiveness across specific learning objectives revealed consistently strong outcomes in ethics, policy, and legal domains (see Table 2). The qualitative data suggested that the scenarios' ability to capture student interest (M = 4.65, SD = 0.49) translated directly into improved perceived understanding, with students frequently citing the realistic nature of the scenarios and their relevance to contemporary issues as key factors in their engagement.

Table 2: Percentage of students who rated the case studies as 'Extremely effective,' 'Very effective,' or 'Moderately effective' in addressing each topic.

Topic	% Effective	*n*
Ethics	95.7	23
Policy	91.3	23
Law	91.3	23

Note. Effectiveness ratings reflect the percentage of students who selected "Extremely effective," "Very effective," or "Moderately effective" on a 5-point Likert scale.

Student feedback on the posthuman aspects of the scenarios emerged as a prominent theme in the qualitative analysis. Many students independently commented on the novel dynamics of learning through AI-generated materials, with a significant portion specifically noting how this approach challenged their preconceptions about human-AI interaction in educational contexts.

9. CONCLUSION AND FUTURE STUDY

The AI-assisted scenario development process and subsequent pilot implementation reveal more than merely the effectiveness of a novel pedagogical tool, demonstrating the emergence of cognitive assemblages between human and artificial intelligence in educational content creation and entanglement. Our findings suggest that this collaborative relationship transcends traditional notions of AI as a mere instrument, instead pointing toward transversal connections (Ferrando & Braidotti, 2019) across human and technological domains in the co-creation of knowledge. For instance, the observed high levels of participant engagement (see Table 1) lend empirical support to the concept of intra-action, wherein participants and the AI-generated content actively shape the resultant learning experience. Similarly, the enhanced comprehension of complex ethical concepts (M = 4.26, SD = 0.81) suggests the emergence of posthuman ethical assemblages, where ethical knowledge is collaboratively constructed through the interplay of human learners and AI.

The empirical evidence from our pilot implementation corroborates this theoretical framework. Students' consistently positive engagement with AI-generated scenarios (Table 1) demonstrates not just pedagogical effectiveness, but an intuitive grasp of intra-action: the mutual constitution of entities through their relationship rather than their pre-existence as separate elements. This was particularly evident in student responses that highlighted how the integration of AI-generated perspectives enhanced their understanding of complex cybersecurity situations, suggesting an emergent form of distributed cognition between human learners and technologically-mediated scenarios.

The scenarios' particular effectiveness in conveying complex ethical concepts merits special attention from a posthuman perspective. Rather than treating AI as a neutral tool for delivering pre-existing ethics education content, our findings suggest that the human-AI collaborative approach created what we might call posthuman ethical assemblages: learning environments where ethical understanding emerges through the dynamic interaction between human learners, AI-generated content, and the technological infrastructure that enables their interaction. The strong student engagement with these ethical scenarios (95.7% agreement, see Table 2) suggests that posthuman pedagogical approaches may be particularly well-suited for exploring the ethical dimensions of contemporary socio-technical systems.

Beyond traditional measures of effectiveness, our pilot implementation revealed how AI-generated scenarios challenge conventional boundaries between human and machine agency in educational contexts. Students' sophisticated engagement with the posthuman aspects of the scenarios—often unprompted—suggests an emerging awareness of how human cognition co-evolves with technological development (Adams & Thompson, 2016). This co-evolution was evident in how students navigated between human and AI-generated perspectives, developing posthuman literacy in their ability to critically engage with both human and machine-generated content.

However, the challenges uncovered during the implementation phase–specifically, instances of AI "hallucinations" and the injection of advanced

terminology outside the scope of the assignment–underscore key considerations regarding the inherent negotiations between human and non-human agency within a posthumanist pedagogy. These issues are not merely technical obstacles but rather manifestations of this ongoing negotiation between human and non-human agencies in educational contexts (Snaza et al., 2014). Addressing these challenges requires not just practical solutions but a theoretical framework that acknowledges the complex interplay between human cognition, artificial intelligence, and pedagogical practice.

Based on our findings, future research has opportunities across critical areas through a posthuman lens. For example, comparative analyses of learning outcomes derived from AI-generated versus traditional case studies should be prioritized, with a specific focus on the qualitative distinctions in participant engagement with human and AI-generated content. This should be done through a posthumanist analytical framework, emphasizing concepts of agency and distributed cognition. Second, longitudinal studies tracking student engagement and comprehension should investigate how prolonged exposure to posthuman pedagogical environments affects learning processes and outcomes. Finally, further inquiry into the discernible differences between authentic and fabricated scenarios is warranted to understand how the constructs of authenticity and simulation mediate participant learning and knowledge construction within posthuman learning environments. A postphenoemnological approach is especially well suited to this.

Though this study is small in scale and relies on self-reported data, it offers significant implications for cybersecurity education and the broader field. It points to the effectiveness of human/AI entanglement directed toward developing and teaching complex ethical concepts, suggesting a transformative approach to curricular development in cyber ethics in particular. Rather than treating AI as simply a tool to be studied, this approach positions it as an active participant with which one negotiates, supporting challenges to traditional notions of agency and expertise in cyber education context. This explicitly aligns with the evolving landscape of cybersecurity practice, wherein human/AI collaboration is increasingly present and characterizing of professional environments.

This posthuman approach to ethics education in cybersecurity also has a range of potential applications beyond academic settings. In industry training and professional development context, for example, human/AI generated content like this could provide timely, relevant learning opportunities that mirror the rapid pace of change in the domain, where practitioners must turn on a dime to deal with emerging ethical challenges. As such, these findings contribute to addressing the workforce development needs identified above. By enhancing student engagement and perceived learning outcomes, these case studies offer a promising approach to attracting and preparing the next generation of cyber professionals, especially in an incredibly complex atmosphere where technical expertise alone is increasingly insufficient.

These findings suggest the potential for fundamentally reconceptualizing how ethical reasoning is taught in technical fields. These case studies, the product of human and AI co-development, represent more than a novel teaching tool. In fact, they serve to exemplify a shift toward posthuman education in the cybersecurity realm, where the boundaries between human and machine, subject and object, become so fluid and negotiable to be almost negligible. This framework acknowledges this distributed and relational nature of ethical decision-making, rather than positioning it as an external constraint on technical practice. The evolution of cybersecurity as a domain stands to position this posthumanist approach in an increasingly vital and valuable role.

10. REFERENCES

Adams, C., & Thompson, T. L. (2016). *Researching a Posthuman World*. Palgrave Macmillan UK. https://doi.org/10.1057/978-1-137-57162-5

Adaryukova, L., Bychkov, O., & Skyrda, A. (2020). The Introduction of Ethics into Cybersecurity Curricula. *CEUR Workshop Proceedings*. https://ceur-ws.org/Vol-2740/20200013.pdf

Austin, G. (2020). Twelve dilemmas of reform in cyber security education. In *Cyber Security Education*. Routledge. https://doi.org/10.4324/9780367822576

Barad, K. (2007). *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning*. Duke University Press. https://doi.org/10.2307/j.ctv12101zq

Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2020). Holistic cyber education. In *Cyber Security Education*. Routledge. https://doi.org/10.4324/9780367822576

Blanken-Webb, J., Palmer, I., Burbules, N., Campbell, R., & Bashir, M. N. (2018). A Case Study-based Cybersecurity Ethics Curriculum. *ASE @ USENIX Security Symposium*. https://www.usenix.org/conference/ase18/presentation/blanken-webb

Cyber Innovation Center, & CYBER.ORG. (2021). *K-12 Cybersecurity Learning Standards*. https://cyber.org/standards

Dexter, S., Buchanan, E., Dins, K., Fleischmann, K. R., & Miller, K. (2013). Characterizing the need for graduate ethics education. *Proceeding of the 44th ACM Technical Symposium on Computer Science Education*, 153–158. https://doi.org/10.1145/2445196.2445245

Ferrando, F., & Braidotti, R. (2019). *Philosophical Posthumanism*. Bloomsbury Publishing Plc. https://www.bloomsbury.com/us/philosophical-posthumanism-9781350059481/

González, A. L., Moreno, M., Román, A. C. M., Fernández, Y. H., & Pérez, N. C. (2024). Ethics in Artificial Intelligence: An Approach to Cybersecurity. *Inteligencia Artificial*, *27*(73), 38–54. https://doi.org/10.4114/intartif.vol27iss73pp38-54

Hayles, N. K. (1999). *How we became posthuman: Virtual bodies in cybernetics, literature, and informatics*. The University of Chicago Press. https://hdl.handle.net/2027/heb05711.0001.001

Jackson, D., Matei, S. A., & Bertino, E. (2023). *Artificial Intelligence Ethics Education in Cybersecurity: Challenges and Opportunities: A focus group report* (arXiv:2311.00903). arXiv. https://doi.org/10.48550/arXiv.2311.00903

Kilhoffer, Z., Zhou, Z., Wang, F., Tamton, F., Huang, Y., Kim, P., Yeh, T., & Wang, Y. (2023). 'How technical do you get? I'm an english teacher': Teaching and learning cybersecurity and AI ethics in high school. *2023 IEEE Symposium on Security and Privacy (SP)*, 2032–2032. https://doi.org/10.1109/SP46215.2023.10179333

Kim, Y. (2016). The Role of Agent Age and Gender for Middle-Grade Girls. *Computers in the Schools*, *33*(2), 59–70. https://doi.org/10.1080/07380569.2016.1143753

Lake, S. (2022). The cybersecurity industry is short 3.4 million workers—that's good news for cyber wages. In *Fortune*. https://fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/

Lin, H. (2022). Influences of Artificial Intelligence in Education on Teaching Effectiveness: The Mediating Effect of Teachers' Perceptions of Educational Technology. *International Journal of Emerging Technologies in Learning (iJET)*, *17*(24), 144–156. https://doi.org/10.3991/ijet.v17i24.36037

Matei, S. A., & Bertino, E. (2023). *Educating for AI Cybersecurity Work and Research: Ethics, Systems Thinking, and Communication Requirements* (arXiv:2311.04326). arXiv. https://doi.org/10.48550/arXiv.2311.04326

National Initiative for Cybersecurity Education (NICE). (2021). *National K12 Cybersecurity Education ROADMAP*. https://www.nist.gov/itl/applied-cybersecurity/nice

Navdeep, A. G. (2022). The Role of Ethics in Developing Secure Cyber-Security Policies. *Tuijin Jishu/Journal of Propulsion Technology*, *43*(4), 250–254. https://doi.org/10.52783/tjjpt.v43.i4.2346

O'Halloran, K. (2020). A posthumanist pedagogy using digital text analysis to enhance critical thinking in higher education. *Digital Scholarship in the Humanities*, *35*(4), 845–880. https://doi.org/10.1093/llc/fqz060

Orchard, R. K. (2019). Using Homemade, Short, Fictional Cases for Teaching the Theory of Constraints. *INFORMS Transactions on Education*, *19*(2), 81–88. https://doi.org/10.1287/ited.2017.0190

Osborne, T., & Rose, N. (2024). Against Posthumanism: Notes towards an Ethopolitics of Personhood. *Theory, Culture & Society*, *41*(1), 3–21. https://doi.org/10.1177/02632764231178472

Pinchot, J., Cellante, D., Mishra, S., & Paullet, K. (2020). Student Perceptions of Challenges and Role of Mentorship in Cybersecurity Careers: Addressing the Gender Gap. *Information Systems Education Journal (ISEDJ)*, *18*(3), 44–53. https://files.eric.ed.gov/fulltext/EJ1258205.pdf

Rowland, P., Podhradsky, A., & Plucker, S. (2018). CybHER: A Method for Empowering,

Motivating, Educating and Anchoring Girls to a Cybersecurity Career Path. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 3727–3735. http://hdl.handle.net/10125/50358

Snaza, N., Appelbaum, P., Bayne, S., Carlson, D., Morris, M., Rotas, N., Sandlin, J., Wallin, J., & Weaver, J. A. (2014). Toward a Posthuman Education. *Journal of Curriculum Theorizing*, *30*(2), 39–55. https://journal.jctonline.org/index.php/jct/article/view/501

Triplett, W. J. (2023). Addressing Cybersecurity Challenges in Education. *International Journal of STEM Education for Sustainability*, *3*(1), 47–67. https://doi.org/10.53889/ijses.v3i1.132

Veletsianos, G., Houlden, S., & Johnson, N. (2024). Is Artificial Intelligence in Education an Object or a Subject? Evidence from a Story Completion Exercise on Learner-AI Interactions. *TechTrends*. https://doi.org/10.1007/s11528-024-00942-5

Wallin, J. J. (2017). Pedagogy at the brink of the post-anthropocene. *Educational Philosophy and Theory*, *49*(11), 1099–1111. https://doi.org/10.1080/00131857.2016.1163246

Wang, P. (2022). Cybersecurity Ethics Education: A Curriculum Proposal. In S. Latifi (Ed.), *ITNG 2022 19th International Conference on Information Technology-New Generations* (pp. 155–159). Springer International Publishing. https://doi.org/10.1007/978-3-030-97652-1_19

Wang, X., & Bai, Y. (2022). Introducing Penetration Test with Case Study and Course Project in Cybersecurity Education. *Journal of The Colloquium for Information Systems Security Education*, *9*(1), 6–6. https://doi.org/10.53735/cisse.v9i1.148

Woodward, A. (2023). Postinformational Education. *International Journal of Philosophical Studies*, *31*(4), 501–521. https://doi.org/10.1080/09672559.2023.2290548