ISSN: 2473-4901
v10 n6144

Teaching Case:

Preparing Posthumanist Perspectives on AI-Human Collaboration in Developing Cyber Ethics Curricula

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
College of Applied Science and Technology
University of Arizona
Tucson, AZ 85721

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 explores the potential, creation, and implementation of AI-generated case studies and scenarios as a novel pedagogical approach to teaching cyber ethics. A scenario development process using generative AI was used to create engaging learning materials for a cybersecurity ethics course. The collaboration between humans and AI resulted in scenarios that address key concepts, promote critical thinking, and offer benefits such as adaptability to learning preferences and relevance to contemporary issues. Challenges like the use of advanced terminology are addressed. Posthuman inquiry, the framework this work is in preparation for applying, opens avenues to explore the diminishing boundaries between human and non-human entities in education. This study contributes to the discourse on AI, cybersecurity, and education, highlighting innovative pedagogical approaches. Further research will investigate the differences between using actual case studies and realistic but fabricated scenarios, contributing to evidence-based strategies for teaching cyber ethics.

Keywords: case studies, scenarios, artificial intelligence, posthuman inquiry, ethics, teaching

1. INTRODUCTION

The integration of artificial intelligence (AI) into cybersecurity practices has brought ethical considerations to the forefront. As cybersecurity professionals encounter complex ethical dilemmas that can shape societies' and cultures' future, ethical principles in AI play a crucial role in guiding the responsible development and implementation of AI systems (Blanken-Webb et al., 2018; López et al., 2024). With the significant shortage of qualified cybersecurity professionals globally, estimated at 3.4 million in 2022 (Lake, 2022) leading to increased workforce demand, the attention paid to cybersecurity education is increasingly crucial, with ethics being a necessary aspect (Matei & Bertino, 2023; P. Wang, 2022). However, the integration of ethics into cybersecurity education is not without its challenges, as cybersecurity specialists may face unpredictable ethical dilemmas not supported by existing laws or codified standards (Adaryukova et al., 2020). This absence of definitive guidelines underscores the necessity for novel pedagogical approaches in cyber ethics education.

A natural starting point is the established learning benchmarks and standards. The K-12 Cybersecurity Learning Standards, developed by CYBER.ORG (2021), provide a comprehensive framework for introducing students to foundational cybersecurity concepts and equipping them with the technical skills and knowledge needed to pursue cybersecurity careers. Similarly, the National K12 Cybersecurity Education Roadmap establishes a coordinated, coherent portfolio of national K12 cybersecurity education activities to ensure effective and efficient deployment of efforts and assets for the greatest potential impact (National Initiative for Cybersecurity Education (NICE), 2021). Likewise, post-secondary cyber education guidance is offered by the National Security Agency's (NSA) Centers of Academic Excellence designations, with the goal of establishing "standards for cybersecurity curriculum and academic excellence" (National Security Agency/Central Security Service, 2024). These initiatives demonstrate the growing recognition of the importance of cybersecurity education and the need for innovative approaches to engage students and promote diversity in the field. Likewise, the development of AI-focused standards by the National Security Agency (NSA) in 2024 point toward the fundamental integration of AI into all cyber-related fields, especially education.

Developing practical applications from theoretical AI ethics principles is a significant issue, and the lack of formal ethical training and clear ethical criteria for educating future cybersecurity experts is a concern (Jackson et al., 2023). These challenges underscore the necessity for novel approaches to its teaching. One such approach is the use of authentic, realistic AI-generated case studies and scenarios, which can provide students with dynamic and engaging learning experiences. This paper explores the potential, creation, and implementation of AI-generated case studies and scenarios in teaching cyber ethics given the current state of cybersecurity education, the need for diverse and inclusive approaches, and the implications of AI for pedagogy.

2. LITERATURE REVIEW

Cybersecurity education should be holistic, integrating technical and non-technical content, and taught in a research-based manner (Austin, 2020; Blair et al., 2020; Sobiesk, 2020). Ethics within the cyber domain is a highly needed but complex topic, as it requires broad balance like security versus civil rights, there is a constant and persistent need to revisit due to technological progress, and, as such, it often drives policy (Navdeep, 2022). Existing teaching cases in cyber education have incorporated ethics into cybersecurity curricula to help students develop ethical awareness and decision-making skills (Adaryukova et al., 2020; P. Wang, 2022). These initiatives demonstrate the growing recognition of the importance of such an integration. However, memorizing laws and codes of ethics alone does not constitute sufficient ethics education for cybersecurity, itself under-studied and under-discussed (Blanken-Webb et al., 2018; Dexter et al., 2013). To address these limitations, innovative pedagogical approaches that engage students in realistic ethical decision-making scenarios are needed.

Scenario- and case study-based education for technical cyber skills like penetration testing has proved effective in introducing major domain concepts (X. Wang & Bai, 2022). It has also been shown to be effective in the domain of cyber ethics education, as they provide students with practical experience in analyzing ethical dilemmas in cybersecurity, immersing them in realistic scenarios and fostering ethical reasoning skills (Adaryukova et al., 2020; Blanken-Webb et al., 2018). Similarly, interactivity and game-based learning has also been found to be an effective method of increasing awareness and interest in cybersecurity and cybersecurity careers (Triplett, 2023). However, curricula constraints, like time restrictions and lack of ready-to-use resources,

can hinder this (Kilhoffer et al., 2023). Early and structured ethical training related to AI use in cybersecurity is needed to address the gap between students' perceived and actual ethical preparedness (Matei & Bertino, 2023).

Beyond this, the field of cybersecurity education also faces challenges in terms of diversity and inclusion. Women are underrepresented in the cybersecurity field (Pinchot et al., 2020), and novel methods should be used to increase recruitment of K-20 females into cybersecurity (Rowland et al., 2018). Girls perform better when learning includes socialization and frequent interaction (Kim, 2016), and peer mentorship is key in cybersecurity programs for both women and men (Pinchot et al., 2020).

The integration of AI in education raises important questions about the nature of learning and the role of technology in shaping educational experiences. While much of the literature on AI in education imagines AI as a tool in the service of teaching and learning (Veletsianos et al., 2024), this focus may not fully account for the complex relational interactions already in process between humans and AI (Woodward, 2023). As AI systems become more advanced, they may potentially develop consciousness or sentience, raising questions about granting them certain protections and responsibilities associated with personhood (Osborne & Rose, 2024). However, current AI systems still have major limitations when compared to human capabilities, and companies like Google strongly refute assertions that their advanced language models have achieved any form of sentience (Osborne & Rose, 2024). The future of AIs as virtual and persistent pedagogical agents remains as likely as not (Straight & Yowika, 2023), driving the need for constant and consistent reconsideration of educational approaches involving AIs.

The successful integration of AI in education also depends on teachers' perceptions of educational technology and their willingness to change traditional methods (Lin, 2022). Students also need training and time to effectively utilize AI-assisted learning. AI-powered text analysis tools can be utilized in innovative pedagogical approaches (O'Halloran, 2020), and story completion methods can uncover hidden truths from participants and invite participant control and creativity (Veletsianos et al., 2024).

As education faces rapidly accelerating changes, it is essential to consider new ways of thinking and teaching (Wallin, 2017). By providing students with realistic and engaging learning experiences, AI-generated case studies and scenarios can help students develop the ethical awareness and decision-making skills needed to navigate the complex ethical dilemmas they may face as cybersecurity professionals (Adaryukova et al., 2020; Blanken-Webb et al., 2018).

3. METHODOLOGY

The course, titled Cyber Ethics, is designed to provide students with a comprehensive understanding of the ethical, legal, and policy implications in the cyber domain, while aligning with the NSA's required knowledge units for a Center of Academic Excellence in Cyber Operations (CAE-CO). The course is structured into seven modules, six of which have associated scenarios, each focusing on a specific aspect of the domain. The learning objectives for each module are aligned with CAE-CO requirements and mapped to each assignment.

To create engaging and thought-provoking scenarios for each module, an AI-assisted scenario development process was utilized, leveraging the capabilities of the Claude 3 Opus model. Claude is the generative AI model developed by Anthropic, Inc., and is similar to the more well-known ChatGPT by OpenAI. The AI was provided with guidelines outlining the learning objectives, key concepts, and desired complexity level for each module. Collaborators, consisting of one graduate student (JL) and two undergraduate students (WY and DP), played a crucial role in providing feedback and guidance throughout the scenario development process.

The AI generated an initial set of scenarios based on the provided guidelines, which were then reviewed by the collaborators. The collaborators provided insights and suggestions for improvement based on their experiences as students in the course (JL and WY) or as potential students (DP). Their feedback focused on assessing the relevance, clarity, engagement level, and alignment of the scenarios with the learning objectives.

Incorporating the collaborator feedback, the AI refined the scenarios to effectively address the key concepts and learning objectives of each module. This iterative process of generation, feedback, and refinement continued until a final set of scenarios was developed for each module, representing a symbiotic collaboration between human and artificial intelligence.

4. SCENARIO DEVELOPMENT

The AI-assisted scenario development process

enabled the quick and efficient creation of diverse scenarios tailored to the specific 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 around the ethical, legal, and policy considerations in the cyber domain.

The cybersecurity ethics, law, and policy course is organized into seven modules, each addressing a specific aspect of the subject matter. Six of these have had scenarios developed, leaving out the initial introduction module that focuses on philosophical foundations of ethics and includes the course introduction. The learning objectives for each module align with the NSA's knowledge unit requirements, ensuring that students gain a comprehensive understanding of the ethical, legal, and policy implications in the cyber landscape.

- **Module 2** introduces 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** examines the legal landscape governing cybersecurity, exploring relevant laws, regulations, and judicial precedents.
- **Module 4** focuses on the policy aspects of cybersecurity, discussing the roles and responsibilities of various stakeholders, such as governments, organizations, and individuals, in shaping cybersecurity policies.
- **Module 5** addresses the ethical and legal implications of privacy and data protection within the context of cybersecurity, a critical topic in the digital age.
- **Module 6** examines the ethical and legal considerations surrounding cybercrime and cybersecurity incidents, including issues such as attribution, jurisdiction, and response mechanisms.
- **Module 7** explores the future trajectory of cybersecurity ethics, law, and policy, considering the potential impact of emerging technologies and the evolving threat landscape.

The AI-assisted scenario development process was employed for each module to generate engaging and thought-provoking scenarios that facilitate student learning and stimulate insightful discussions. The AI model chosen, Claude 3 Opus, was provided with guidelines outlining the learning objectives, key concepts, and desired complexity level for each module. The generated scenarios were designed to be realistic and relevant, drawing inspiration from authentic, contemporary issues and obstacles in the field of cyber. For example, in Module 5, a scenario was generated that explored the legal and ethical implications of a fictional smarthome device company that has been secretly collecting and sharing user data with third-party advertisers and government agencies. This scenario challenges students to consider the responsibilities of organizations in safeguarding user data, the potential consequences for affected individuals, and the appropriate response measures.

Throughout the scenario development process, the student authors played a vital role, providing valuable feedback and guidance. Their insights, based on their experiences as students in the course or as prospective students, facilitated the refinement of the scenarios, ensuring that they effectively addressed the learning objectives and promoted engagement. The final set of scenarios for each module represents the outcome of an iterative process of generation, feedback, and refinement. The collaborators' input was instrumental in shaping the scenarios, making them more relevant, clear, and engaging for the students. The AI's ability to incorporate this feedback and generate refined scenarios demonstrated the potential of AI-assisted scenario development in creating effective learning materials for cyber ethics, law, and policy.

Scenarios were designed to be dossier-like, including an overview, a range of background and supplemental information, "main characters" that acted as individuals of interest and major players throughout, and a timeline of social media posts, news stories, internal emails, and so on. Not only did this provide students with a realistic view of the case in question but allows for the integration of other cyber-related skills like open source intelligence gathering while requiring deep, critical readings and cross-referencing of materials. Below is an outline of these for the Module 6 scenario described above (note that social media site clones are used; SocialPark mimicking Facebook, ChirpyHub mimicking Twitter/X, et cetera):

Background Documents

1. HomeTech_PrivacyPolicy.pdf
2. SmartHomeDevices_PrivacyRisks.pdf
3. DataSharingAgreement_Excerpt.pdf

Individuals

1. Rachel Evans (HomeTech CEO)
   Username: @RachelEvans

Company: HomeTech
2. Jason Kim (Privacy Advocate)
Username: @JasonKim
Company: Consumer Privacy Rights Organization
3. Dr. Lila Patel (Cybersecurity Expert)
Username: @DrLilaPatel
Company: IoT Security Standards Board
4. Senator Ethan Roberts (Policymaker)
Username: @SenatorRoberts
Company: United States Senate
5. Sophia Clarke (Concerned Consumer)
Username: @SophiaClarke
Company: N/A

Websites
• HomeTech corporate website
• Consumer Privacy Rights Organization
• IoT Security Standards Board

Social Media Interactions
• HomeTech press releases and statements on SocialPark
• Privacy advocates discussing concerns on ChirpyHub
• Policymakers debating regulation on ChirpyHub

5. TEACHING GUIDE

Despite the relative ease and speed of the current incarnation of generative AI, integrating the AI-generated scenarios into the curriculum and classroom requires careful planning and facilitation to ensure that students engage in meaningful discussions and develop a deep understanding of the domain. In concert with the provided supplemental materials, the following brief teaching guide describes the process for incorporating the scenarios into the course, including discussion questions, activities, and strategies for facilitating productive conversations.

Begin by introducing each scenario within the context of the corresponding module's learning objectives. This approach helps students understand the relevance of the scenario and the key concepts they should focus on. Provide a concise overview of the scenario and introduce its main characters or stakeholders to set the stage for the discussion.

Discussion questions are a critical component of the teaching guide, as they encourage students to engage in critical thinking about the scenario and explore its ethical, legal, and policy dimensions. For each scenario, a set of open-ended questions should be carefully developed, prompting students to consider the perspectives of diverse stakeholders, analyze the potential consequences of various courses of action, and evaluate the scenario through the lens of ethical frameworks and legal principles.

In addition to discussion questions, include activities that enable students to actively engage with the scenario and apply their knowledge. For example, 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 work in small groups to develop guidelines or recommendations for addressing the ethical, legal, or policy challenges presented in the scenario.

To facilitate meaningful discussions, it is essential to create a safe and inclusive learning environment where all students feel empowered to share their thoughts and perspectives. Establish ground rules for respectful dialogue and encourage active listening to foster a productive conversation. As the instructor, guide the discussion, clarify concepts when necessary, and ensure that all students have the opportunity to contribute.

When facilitating discussions, draw connections between the scenarios and real-world events or current developments in the cybersecurity domain. This approach helps students understand the relevance and applicability of the concepts they are learning. Encourage students to share their personal experiences or insights related to the scenario to further enrich the discussion and promote peer-to-peer learning. The development and use of fictional–which is to say realistic but not real–case studies and scenarios has been shown to be effective for fostering engagement and drawing varied student responses (Orchard, 2019).

Finally, provide students with resources for further learning and exploration, such as additional 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. To illustrate the impact and expectations such AI-generated scenarios can have, the student co-authors of this work–who also assisted in the development of scenarios–provide the following perspective.

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, innately 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.

All considered, 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. CONCLUSION AND FUTURE STUDY

The AI-assisted scenario development process, leveraging the capabilities of generative AI and the insights of student collaborators, demonstrates the potential for creating engaging, relevant, and thought-provoking learning materials. Collaboration between human and artificial intelligence has resulted in scenarios that effectively address key concepts and learning objectives while promoting critical thinking and meaningful discussions.

The benefits of AI-generated scenarios are numerous and made plain here, including adaptability to different learning preferences, relevance to contemporary issues in cybersecurity, and the ability to captivate students' interest. By providing students with realistic and immersive contexts to explore complex ethical, legal, and policy considerations, these scenarios contribute to the development of essential skills and knowledge for future cybersecurity professionals.

Further, the aforementioned collaboration between human and artificial intelligence in the development of such AI-generated scenarios raises important questions about the nature of this relationship and its potential implications for the field of education. Approaching this through the lens of posthumanism, avenues open to challenge traditional notions of human exceptionalism and explore the diminishing boundaries between human and non-human entities (Adams & Thompson, 2016; Snaza et al., 2014).

Engaging with AI in the creation of educational content itself represents this shift towards a posthumanist approach to teaching and learning. As AI systems become more sophisticated and capable of generating content that is indistinguishable from human-created materials, the traditional roles of teacher and student, as well as the concept of expertise, may be challenged and redefined. This posthumanist perspective offers a framework for exploring the transformative potential of human-AI collaboration in education and its implications for the future of knowledge production and

dissemination.

It is important, however, to acknowledge the challenges associated with AI-generated scenarios, such as the potential use of advanced terminology that may hinder student comprehension and the inclusion of "hallucinations" not based in reality (for example, the inclusion of fabricated websites, articles, et cetera). Addressing these challenges through the comprehensive development of realistic, broad support materials is crucial to ensure the effectiveness of this approach. It is important to bear in mind that the application of these AI-driven scenarios is currently work in progress, and the intervention has not yet been applied to a classroom setting. The authors intend to conduct additional studies to investigate the appreciable and pedagogically-beneficial differences between using actual case studies and realistic, fabricated scenarios. These investigations will contribute to the development of evidence-based intervention strategies and best practices for using AI-generated scenarios in the teaching of cyber ethics.

A full and comprehensive guide to developing, implementing, and evaluating these scenarios will be released in the future. This guide will serve as a valuable resource for educators and institutions seeking to incorporate AI-generated scenarios into their cybersecurity curricula, providing a practical framework for creating effective learning materials that address the unique challenges of teaching cyber ethics in an ever-evolving technological landscape.

The use of AI-generated case studies and scenarios points toward a promising approach to teaching cyber ethics, offering a powerful tool for engaging students and fostering the development of essential skills and knowledge. As the field of cybersecurity continues to evolve, the integration of artificial intelligence in education will play an increasingly vital role in preparing future professionals to navigate the complex ethical challenges they will face. This study seeks to contribute to the ongoing discourse on the intersection of AI, cybersecurity, and education, highlighting the potential for innovative pedagogical approaches to shape the future of the field.

8. 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.

Austin, G. (2020). Twelve dilemmas of reform in cyber security education. In *Cyber Security Education*. Routledge.

Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2020). Holistic cyber education. In *Cyber Security Education*. Routledge.

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.semanticscholar.org/paper/A-Case-Study-based-Cybersecurity-Ethics-Curriculum-Blanken-Webb-Palmer/456e7c76d490b304750a2377843e70d9d2f0cb33

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

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

ISSN: 2473-4901
v10 n6144

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

López, A., Moreno, M., Moreno, A., Hadfeg, Y., & Cepero, N. (2024). Ethics in Artificial Intelligence: An Approach to Cybersecurity. *Inteligencia Artificial, 27*(73), 38–54. https://doi.org/10.4114/intartif.vol27iss73pp38-54

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

National Security Agency/Central Security Service. (2024). *Centers of Academic Excellence*. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

Navdeep, A. G. & Muskan, V. S. (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.

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.

Sobiesk, E., Andrew O. Hall. (2020). Educating future multidisciplinary cyber security teams. In *Cyber Security Education*. Routledge.

Straight, R., & Yowika, W. (2023). From Parasocial to Posthuman: (Virtual) Pedagogical Agents, Parasocial Phenomena, and the Future of Immersive Learning. *Proceedings of EdMedia + Innovate Learning*, 1–6.

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