Article Analysis

Bakarri Grant
8/8/2025

Introduction

This article, “*Integrating Humanities into Cybersecurity Education: Enhancing Ethical, Historical, and Sociopolitical Understanding in Technical Training,”* by Frusci (2024) delivers a message that cybersecurity education must go beyond teaching purely technical skills to include the ethical, historical, and sociopolitical contexts in which cyber activities occur. By merging humanities-based learning with technical training, the study argues that students develop into well-rounded professionals who can understand not only how to secure systems but also why such security matters to society, policy, and human well-being. This study reflects a growing recognition in the field that cybersecurity challenges are as much about people, institutions, and values as they are about code and hardware.

Relation to social science principles

Frusci explicitly frames cybersecurity education as interdisciplinary, weaving in ethics, sociology, political science, history, law, and anthropology to situate technical skills within human systems and institutions. The rationale is that modern cyber issues are sociotechnical and demand ethical reasoning, historical perspective, and policy literacy.

Research questions, hypotheses, and methods

This study asks whether integrating humanities content into high school cybersecurity courses improves students’ technical knowledge, ethical reasoning, historical understanding, and sociopolitical awareness. The abstract mentions these and develops them as the paper's outcome measures. With the research question above in mind, Frusci developed a pilot cybersecurity course for 12th grade students that incorporated humanities disciplines and aligned with the *New York State K-12 Computer Science and Digital Fluency Standards.* The goal of the course was to encourage students to think beyond technical solutions and consider the broader implications of their actions in a complex and interconnected world.

Data and Analysis

Quantitative Data Collection: Students took exams at the beginning and end of the course. The aim was to establish a baseline of their understanding of cybersecurity concepts and measure their progress at the end of the course. Rubric-based assessments were used to evaluate their ability to synthesize technical, ethical, historical, and sociopolitical perspectives. Students then completed surveys at the end of the course to measure their perceived growth in understanding the material. Surveys included close-ended Likert scale questions and open-ended questions for deeper reflection.

Quantitative data from the pre/post exams and rubric-based assessments were analyzed using descriptive statistics to measure changes in students' performance. To quantify the students' growth, mean scores, standard deviations, and percentage improvements for each of the four categories were calculated. Rubric outcomes (Final Projects) show improvements across the four categories.

Qualitative Data Collection: Data was collected from reflection papers, open-ended survey responses, and semi-structured interviews. This was to gain insight into the students' experiences with the course and their perceptions of how the interdisciplinary approach influenced their learning.

This data was analyzed using thematic analysis, coding student responses to identify key themes related to ethical reasoning, historical understanding, and sociopolitical awareness. Reflection papers identified common themes like increased ethical awareness, the ability to contextualize cybersecurity within historical events, and the recognition of global sociopolitical dynamics.

Links to Class Concepts

There are many concepts of this article that relate to topics we've discussed in class. The course covers theories like social norms theory, routine activities theory, and criminological frameworks to understand how human behavior contributes to cyber threats. The curriculum in the article applies these ideas by teaching students to examine attacker motives, societal impacts, and human factors. This application connects social science theories to real-world cyber threats. We've recently learned how cyber incidents affect different social groups in varied ways, often amplifying existing inequalities. Frusci notes that cyberattacks' impacts vary across communities, highlighting digital literacy gaps and unequal access to resources. This discussion directly aligns with the class focus on equity and inclusion in cyber policy and practice. The last connection that I'd like to make is the emphasis that cybersecurity problems aren't just technical; they are shaped by social, cultural, and political contexts. Frusci's article mirrors this by integrating history, ethics, and sociopolitical analysis into technical cybersecurity education. This reinforces the idea that understanding people, institutions, and values is essential for effective security practices.

Marginalized Groups

While this article does not focus specifically on a marginalized population, its sociopolitical framing and claim that attacks affect different communities in "varied ways" highlight equity implications—e.g., how disparities in digital literacy or institutional capacity shape risk and recovery. This framing supports curricula that reveal which groups benefit or lose under various cyber policies and practices.

Societal Contributions

The study contributes an evidence-based model for humanities-based cybersecurity education that measurably increases ethical reasoning and broader civic/policy literacy competencies society needs from the next cyber workforce. It offers actionable curriculum components and reports documented learning gains, strengthening the case for scaling interdisciplinary cyber programs in K-12 and beyond.

Conclusion

Frusci’s study shows that bringing social science into cyber isn’t fluff; it’s measurably effective. Students got better not only at the what (technical content) but also at the why (ethics, history, policy, social impact). That combination is exactly what organizations and a healthy digital society need.

References

Frusci, J. (2024). Integrating Humanities into Cybersecurity Education: Enhancing Ethical, Historical, and Sociopolitical Understanding in Technical Training. Journal of Cybersecurity Education, Research and Practice, 2024(1), Article 31. https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/31