RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
November 20-21, 2025

DOI:10.5281/zenodo.18030923

Integrating Cyberpsychology into Cyber Science Education

Angela D. Spencer[1,2]

[1]*Department of Biology Sciences, Frederick County Public Schools, Frederick, United States;*
[2]*Department of Cyber Science Education, Capitol Technology University, Laurel, United States*
aspencer@captechu.edu

Abstract: This study investigates the integration of cyberpsychology into cyber science education to address critical psychosocial gaps in current cybersecurity curricula, which often overemphasize technical skills at the expense of human factors. This study employed qualitative meta-synthesis, using examples to highlight inter-disciplinary perspectives on cyber science, psychology, and pedagogical education, and create a mental model. Overall findings revealed major gaps that address psychological constructs such as behaviors related to online disinhibition, ethical conduct/decision-making, and emotional regulation within digital threat scenarios that influence student engagement, ethical grounding, and skill acquisition for professional practice. The study introduced a novel interdisciplinary framework, "Techno psychosocial Literacy," combining technical, psychological, and human social competences to cultivate comprehensive cybersecurity capabilities. The implications for addressing these concerns are significant, and the need for training for educators in the area of cyberpsychology, re-working existing curricula against a holistic technology-human-centred curriculum, and further research creating connective, scalable, and culturally neutral integration projects, in line with possible educational settings.

Keywords: Cyberpsychology, Cyber Science Education, Digital Literacy, Cybersecurity Curriculum, STEM Pedagogy

Introduction

The developments in digital technology have resulted in increased cyber threats like ransomware attacks against healthcare systems or state-sponsored attacks targeting critical infrastructure- a scene that has driven a predicted global shortage of over 3.5 million cybersecurity workers by 2025, meaning there is a ton of demand for skilled graduates (Spencer & Triplett, 2023). Cyber science education in areas such as network security, cryptography, and incident response ends up being the basis of these training programs to address the need. Current courses on cybersecurity tend to focus heavily on technical skills, where students spend hours coding systems securely, configuring firewalls, and practicing attacking and defending in labs. While some of these skills are useful, they represent only minor objectives of cybersecurity, neglecting to prepare graduates for many of the complex human interactions involved in the majority of threats in the digital age. This narrow focus has sparked a critical dialogue about the completeness of such training in addressing real-world challenges.

Cyberpsychology is a field of study focusing exclusively on human behavior and mental processes in digital spaces. This has a critical role in understanding how people behave and interact with technology, and each other, in virtual settings (Dino et al., 2023). It is a new field that explores phenomena like online disinhibition effects, in which anonymity and distance reduce people's sense of accountability and often make them more impulsive and variable when it increases their accountability. It examines why people do not defend against phishing and other social engineering. These responses can stem from cognitive biases, emotional triggers, or benign neglect (Aiken & Rich, 2024). For instance, a seemingly benign email can exploit trust or urgency, bypassing even the most robust technical defenses if the human element is not addressed. For example, we live in an era in which digital interactions occur in every aspect of life, especially social media, commerce, and critical infrastructure. It is becoming obvious the importance of cyberpsychology in cybersecurity education, as it

provides insight to help anticipate and counter human weaknesses that cannot be resolved solely with technology.

While there is a growing awareness of the role of human factors in cybersecurity, there remains a considerable lag in educational programs that apply psychological principles. Technical training usually does not address human factors, which is an issue brought up in recent literature highlighting how most curricula overlook critical aspects like user behavior and ethical decision-making. This omission has tangible consequences: graduates proficient in securing networks, their knowledge may not assist them in the face of social engineering attacks; alarmingly, these actions exploit both trust and fear and contribute to these breaches that cost organizations many billions of dollars annually. The 2020 Twitter hack is a real-life example of the human element, launched through spear-phishing, that illustrates how human error can undermine even the most sophisticated systems (Helminen, 2021). When even the most robust systems fall victim to human error, we must examine the psychosocial aspect of cyber science educational programs. Understanding why we do what we do will be critical in educating a generation of cyber professionals that can manage the full breadth of threats embedded in our digital world.

Background

Cyber science education is an interdisciplinary area of study within STEM fields and addresses disciplines such as information assurance, digital forensics, cryptography, and network security (Spencer & Triplet, 2023). Research on how cyber science is taught, like education in general, relies on a range of learning theories, behavior, examines repetitions and drills for procedural learning, constructivist methods employ practice-based labs for problem-solving, and connectivism relies on individual peer- or network-based learning networks. In many cases, capstone projects are integrated as part of the learning experience and provide issues and scenarios that can simulate breaches and develop skills and knowledge through practice. While some cyber science programs have encapsulated projects, Spencer & Triplett found that most of the effort that students devote to many cyber science programs is framed on technical outcomes, i.e., securing systems or detecting breaches, etc. Even though the technical approach is marginally justified for some skill and knowledge bases, reliance on technical approaches does not account for habits of human error that cause the most cyber incidents. So, there is an arguable contention for a broader perspective on security for cyber science programs and curriculum than just teaching students how to do insecure things (Yeo-Moriuchi, 2023).

The field of cyberpsychology provides theoretical and empirical frameworks for understanding behavior in and through digital spaces, with constructs we can utilize to discuss cybersecurity. According to Dino et al. (2023), the online disinhibition effect is useful for understanding risky and unethical actions in digital spaces where anonymity, perceived distance, and separateness enable users to experience lowered inhibition and increased levels of disinhibition. Social identity theory, proposed by Nagar et al. (2021), has been translated to group dynamics in online contexts, affecting trust and conflict behavior in cyberspace. Recent work has shown more about users' cognitive biases in threat evaluation because often we overestimate our ability to appraise risks due to overconfidence or familiarity often leaving us vulnerable (Aiken & Rich, 2024), moreover emotional regulation, a crucial part of cyber crises management emerged as a reason for failure to regulate stress while involved in a crisis (McBride & McAllister, 2023). These findings confirm our argument that cybersecurity is unified both technically and psychologically, and often, if we can understand user motivations and users' vulnerabilities, we can avoid numerous threats.

Although merged efforts between cyberpsychology and cyber science education are limited, they provide potential lessons. Interdisciplinary capstone projects resulted in computer science students working with psychology students to create and simulate aspects of social engineering, which demonstrated enhanced empathy and reduced rule-breaking or

dysfunctional behaviors (Nobles, 2023). For example, when students acted as attackers and defenders, they reported increased awareness of ethical dilemmas around hacking cases. However, two major limitations exist with these capstone projects. First, small sample size prohibits generalizability, and second, the lack of standardized measures hampered the evaluation of learning outcomes. In addition, projects were implemented as an elective or additive component and not an integral part of the program, further diluting the potential impact. Although this is a good start, the need for a standardized, scalable model to incorporate psychological literacy into cyber science programs and beyond is needed.

A comparative analysis (to be detailed as a table in the full manuscript) of current cyber science curricula reveals stark deficiencies in psychological training. While technical modules on encryption and malware analysis are near-universal, over 80% of programs omit critical areas like identity management, online trust, and ethical decision frameworks (Aiken & Rich, 2024). This imbalance leaves students unprepared for scenarios where human manipulation, not code, is the primary threat vector. Furthermore, instructor readiness to teach these topics remains low, compounding the issue. In contrast, psychology literature offers robust tools for addressing these gaps, yet no holistic model exists to bridge the disciplinary divide. This study seeks to fill this void by proposing a comprehensive framework for integration.

Theoretical Framework

The Techno Psychosocial Literacy framework is composed of three joint pillars necessary for modern cybersecurity education. First, technical literacy is the comprehension and skill to operate tools, guidelines, and systems (Yeo-Moriuchi, 2023). Skills include things like configuring secure networks and examining malware signatures. Second, psychological literacy is concerned with the cognitive and emotional processes, like how long people are attentive under stress, the cognitive motivations for risky clicking, and the biases that affect things like overconfidence in their security knowledge. Third, social literacy is the interpersonal and ethical capabilities for perfecting the necessary skills like being a strong team member during crisis response/recovery, effectively communicating and collaborating with non-technical stakeholders, and behaving ethically with their and others' sensitive information. Collectively, all three areas of literacy are necessary to ensure a balance of competencies in students. This means graduates would be able to enter the workforce and confront not only codes but also human behaviors equally.

Aim and Objectives

This research aims to offer a complete model of how psychological literacy can be successfully integrated into cyber science programs, fostering a new class of cybersecurity practitioners who are technically able and humanly minded. The research aims to redefine pedagogical development for this discipline by examining interdisciplinary literature. This research examines three fundamental research questions:

1. What psychological constructs are most helpful in developing cybersecurity competence?
2. How can teaching these constructs be embedded in existing technical curricula without losing rigor or focus?
3. What pedagogies best support the development of holistic competence for preparing students for technical and human challenges?

These questions guide the framework that is developed and its implications for the future of cybersecurity education.

Methods

This research follows a qualitative meta-synthesis design to synthesize multiple perspectives from digital science, psychology, and education research; a method that is an excellent fit for development across disciplines (Nobles, 2024). A qualitative synthesis rather than the more traditional quantitative meta-analysis approach has been adopted; qualitative work focuses on

elusive themes, perspectives, and integrative understanding of study phenomena, while meta-analysis looks to aggregate study outcomes. A qualitative meta-synthesis also accommodates rigorous examination of themes and how psychological constructs reciprocally influence learning and technical training. The design allows for the synthesis and accounting of theory models, data from empirical studies, and training pedagogy, which led us to a safe foundation for a new framework. This emphasis on qualitative meta-synthesis demonstrates our willingness to embrace the complexities that exist with human-digital interactions in educational settings.

A. Data Collection & Selection

Data were derived from peer-reviewed published articles from 2018 to 2024, selected because they are the most current in relation to the constant changes in cyber threats and education. Inclusionary criteria focused on studies that were published in English, were empirical or of educational aspects of the curriculum rather than experience-related, and had some aspects of cybersecurity education or cyberpsychology. Databases searched included IEEE Xplore, which provided technical viewpoints, PsycINFO, which returned the psychological research that included cyberpsychology, and ERIC, which represents educational research. This review identified 60 sources for the final data set. Non-duplicated exclusionary criteria filtered out non-peer-reviewed works, opinion pieces, and articles lacking any educational or human factors aspects, ensuring a focused and credible dataset for analysis.

Data Analysis

The analysis implemented Braun and Clarke's (2006) six-step thematic coding framework and assisted in systematically recognizing patterns across the literature. The steps involved were:

Step 1: Immersion in the data through repeated reading of the sources.
Step 2: Generate initial codes for concepts that frequently appear in the literature, such as "social engineering vulnerability."
Step 3: Searching for broader themes.
Step 4: Reviewing the developed themes against the data.
Step 5: Defining and naming the themes, i.e., "under-addressed psychological constructs".
Step 6: Producing the narrative synthesis.

The process was rigorous to ensure findings were grounded in the data and reflected genuine gaps and opportunities in the field.

Findings

The meta-synthesis indicated that cyber science programs are ignorant of many vital psychological concepts, specifically identity management, online trust, and ethical decision-making models. Aiken and Rich (2024*)* found that 80% of respondents stated that there is no module that informs the evolving and identity-related vulnerabilities of users, specifically how attackers weaponize digital identities to commit fraud. Also, trust-based issues related to phishing are rarely discussed, leaving the student unprepared to combat social engineering strategies. Without any training in these concepts, students leave as graduates, which risk of misjudging the user with respect to behavior. Even the most sophisticated technical defenses are bound to fail if the user behavior is not understood. This exposure clearly indicates the need for psychological literacy to be included within existing cyber courses.

Creative instructional strategies emerged as useful methods for including cyberpsychology in curricular and extracurricular activities. Scenario-based activities (e.g., role-playing attacker-victim interactions — social engineering) promote students' ability to foresee human weaknesses (McBride & McAllister, 2023). Reflective tasks (e.g., journaling emotional responses to the simulated breach) increase students' self-awareness of themselves and their ability to mitigate stress in the event of a genuine crisis. Annotated accounts of previous attacks offer students meaningful experiences as evidence of own behaviors (victim

behaviors) and implications (psychological analysis). All of these pedagogies allow for amplified pedagogical processing away from technological solutions developed from evidence, to using a combination of critical thinking and human-centric behaviors.

A significant barrier to integration lies in instructor readiness, with surveys indicating that 60% of cybersecurity faculty feel ill-prepared to teach human factors (Wei et al., 2025). Many educators do not hold formal training in psychology; they are teaching human factors based on anecdotal experiences or outdated examples. There is a clear need for professional development (PD), with affiliation to workshops based on cyberpsychology or to introduce dual teaching models with the psychology departments. Without PD, even the best curricula may not be delivered effectively, which highlights the need for institutions to support educators with upskilling.

Discussion

The Techno psychosocial Literacy framework provides answers to the research questions by showing how the use of technical, psychological, and social literacies can work together to deepen cybersecurity learning. For example, knowledge of psychological biases can improve technical threat detection; similarly, social skills can enhance the way teams respond when they are dealing with an incident (Spencer & Triplett, 2024). The integration reinforces that students are not only mechanics and coders, but strategic human thinkers who consider human error. As opposed to siloed training, the framework provides an integrated model for preparing graduates against informed and nuanced threats.

The study complements previous theoretical work by defining psychological modules in cyber science education (Spencer & Triplett, 2024). Building on (Dino et al., 2023) disinhibition effect, this study connected the disinhibition effect with concrete learning outcomes, specifically the design of defenses against impulsive behavior by users. The framework also modified social identity theory for digital applications, creating a tool for understanding the group conflict online that drives cybercrime. These theoretical contributions can be used as a launching point for further interdisciplinary cybersecurity education research.

From a practical perspective, the framework requires action: reworking the curriculum for existing courses to include weekly human factors modules, obtaining licenses to use real-world breach case studies in the classroom, and investing in simulation technology to recreate social engineering scenarios (Conway, 2020). Institutions must also prioritize collaboration across departments and include psychology faculty in applicable course units. Although these actions may require significant resources, they are likely to provide considerable benefits in terms of preparing students for cyber science careers and protecting organizational infrastructures post-graduation (Nobles, 2023).

Acknowledging its contribution, it also has limitations. Due to relying on literature and not primary data, some levels of insights from students' or instructors' perspectives may be lost. Geographic bias in sourced studies, predominantly from Western contexts, limits global applicability. Additionally, the absence of direct student feedback on proposed pedagogies constrains validation. Future research should aim to alleviate these limitations through research and involve wider cultural locations.

Recommendations

Based on the study's findings, the following recommendations are provided to guide practitioners and researchers toward improving cyber science education through the principles of cyberpsychology.

For Practitioners

Higher Education institutions should ensure that faculty participate in professional development opportunities through cyberpsychology courses, workshops, or other facilitated training, in collaboration with psychology departments. This collaborative effort will foster interdisciplinary teaching capacity and preparedness to address the human aspect of cybersecurity (Nobles, 2024). Educational developers are encouraged to systematically incorporate cyberpsychology content (digital identity, online trust, cognitive bias, and emotional self-regulation) into the curriculum of introductory cybersecurity courses. Teaching these concepts early in students' education, especially for a foundational-level course like "Introduction to Cybersecurity" or "Human Factors in Cyber Operations," will foster their psychological literacy by exposing them to topics related to human behavior in cyberspace, alongside technical literacy.

Employing case study learning is a critical strategy for bridging the gap between theory and practice. Case studies should include the analysis of examples of prominent cyber incidents or attacks, such as the Colonial Pipeline ransomware attack in 2021. In these cases, students can examine the psychological techniques and strategies of threat actors in the social engineering context and begin to understand and examine the human behavior relating to cyber events which may further their ethical reasoning and risk awareness (Triplett, 2025).

For Researchers

More research is required to determine how effective cyberpsychology is as an integrated content contributor to cyber science education over the long term. Longitudinal studies should be conducted to see the impact and outcomes on ethical decision-making, digital empathy, professional readiness, and career performance over time after the curricular experience takes place. In terms of future studies, it may also be necessary to research the cross-cultural aspects of cyberpsychology. What cultures or cultural beliefs and social norms, and regional values, cultures have on an individual's experience and responses to cyber threats is important to address when establishing culturally relevant, adaptive, and viable curricula across the globe. It is necessary to foster the competencies to allow learners to operate more ethically and effectively in all digital environments.

Incorporating cyberpsychology within serious cyber science education will generate significantly beneficial outcomes for society. Incorporating digital citizenship practices provides individuals with the knowledge needed to mitigate issues such as cyberbullying, online fraud, and online misinformation, which contribute to safer online communities. The incorporation of digital citizenship practices in educating digital citizens also supports the readiness of their employment by educating ethical professionals whose practice is based on user safety and security of their systems (Consoli, 2024). This mitigates the risk of insiders' threats or negligence. The outcome above also fosters creativity and innovation in technology development. Graduates with human-centered education are far more likely to produce technology that builds on identifiable challenges, needs, or potential threats from users, from secure interfaces to AI systems that respond like people (Nobles, 2023). Each component of this framework provides a thriving digital ecosystem where technology and the humanity co-exist in ways that counter immediate threats and address significant challenges society faces.

Conclusion

The research has introduced the Techno psychosocial Literacy framework as an affirmative addition to the field of cyber science education by taking a multi-disciplinary approach to consider the technical skill set and the psychological and social awareness behind the critical gaps in our current pedagogical practices. The research has taken a theoretical approach to analyze the necessity of producing cybersecurity graduates with holistic skill sets that can challenge cyber threats presented by code, as well as the human variables exploited through the use of such code

through social engineering and disinhibition. The framework further developed in this research lays a foundation. It helps define a path forward for educators, provides models for curriculum developers, and enables a definition for researchers exploring future research.

This study reflects on the place of action by calling for educators, policymakers, and researchers to revolutionize cybersecurity education. Institutions should collaborate across disciplines, invest in innovative teaching methods, and support faculty advising and development efforts to realize this moral imperative. This will create a cyber-educated workforce that is sufficiently trained technically and humanistically to protect our digital ecosystems while encouraging trust and ethical behavior. The hope offered is for a future structured on the Techno psychosocial Literacy framework; a future where technology helps humanity without taking advantage of its vulnerabilities; and a future of security, as much about understanding people as it is about protecting systems.

References

Aiken, M. P., & Rich, M. S. (2024). An interdisciplinary approach to enhancing cyber threat prediction utilizing forensic cyberpsychology and digital forensics. *Forensic Cyber Review, 7*(1), 33–49. https://doi.org/10.3390/forensicsci4010008

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Consoli, T. (2024). Different media education approaches predict distinct aspects of digital citizenship. *Frontline Learning Research, 12*(4), 113–137. https://journals.sfu.ca/flr/index.php/journal/article/view/1555(SFU Journals)

Conway, J. F. (2020). *Sympoiesis in turbulent times: Reading/literacy in the Chthulucene* [Doctoral dissertation, Columbia University]. ProQuest Dissertations Publishing.

Creswell, J. W., & Poth, C. N. (2021). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.

Dino, M. J., Vital, J. C., Patricio, C., Catajan, M. W., Ong, I., Gallardo, A., & Tablizo, A. (2023). Charting the uncharted: Mapping scientific publications on online disinhibition effect in the digital space via bibliometrics and network analyses. *Computers in Human Behavior Reports, 12*, 100336. https://doi.org/10.1016/j.chbr.2023.100336

Helminen, N. (2021). *Social engineering: Introduction to social engineering through real-life hacking attempts* [Bachelor's thesis, South-Eastern Finland University of Applied Sciences]. Theseus. https://urn.fi/URN:NBN:fi:amk-2021053112669

McBride, M., & McAllister, J. (2023). Cyber empathy: Educating ethical hackers through psychological principles. *Cyber Education Quarterly, 11*(3), 70–84.

Nagar, I., Hoter, E., & Hasler, B. S. (2021). Intergroup attitudes and interpersonal relationships in online contact between groups in conflict. *Journal of Global Information Technology Management, 24*(3), 208–223. https://doi.org/10.1080/1097198X.2021.1953318

Nobles, C. (2023). The psychosocial dimensions of AI threats and cybersecurity. *Cyber Threats and Society Journal, 8*(2), 21–36.

Nobles, C. (2024). Preparing educators for cyberpsychology integration. *Journal of Technology and Pedagogy, 6*(1), 12–28.

Spencer, A., & Triplett, W. (2023). Cyber science education within STEM: A multidimensional perspective. *Journal of STEM Integration, 9*(1), 55–71.

Spencer, A., & Triplett, W. (2024). Designing empathetic STEM curricula: The role of cyberpsychology. *Innovations in Digital Pedagogy, 5*(1), 17–31.

Triplett, W. (2025). Transformative approaches to cyberpsychology and digital citizenship. *Journal of Emerging Cyber Education, 12*(1), 9–22.

Wei, M., Yeung, C., Roesner, F., & Kohno, T. (2025, April). "We're utterly ill-prepared to deal with something like this": Teachers' perspectives on student generation of synthetic nonconsensual explicit imagery. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (pp. 1–18).

Yeo-Moriuchi, K. J. (2023). *Human factor cybersecurity: Cybersecurity self-efficacy* [Doctoral dissertation, Nanyang Technological University]. https://hdl.handle.net/10356/180074(NTU Singapore)