CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 5, No. 1
April 2026
ISSN: 2832-1006

In this issue:

iscap
Information Systems & 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.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

2026 Review Board

Enhancing Student Learning in Information Security Courses: Integrating Generative AI, Critical Thinking, and Case-Based Pedagogy

Gary Yu Zhao
zhao@nwmissouri.edu

Cindy Zhiling Tu
cindytu@nwmissouri.edu

Joni Adkins
jadkins@nwmissouri.edu

School of Computer Science and Information Systems
Northwest Missouri State University
Maryville, Missouri, US

Abstract

Generative AI (GenAI) offers transformative potential in higher education, particularly in the information security field. This study explores the integration of GenAI tools into information security courses, proposing a structured framework that enhances critical thinking and problem-solving skills through case-based learning. By combining GenAI with the analytical framework, Motivation-Methods-Resources-Impact-Solutions (MMRIS), we conducted a two-phase case study. In total, 191 graduate students across 32 groups submitted the case study assignment and completed the reflection survey. The results show that 72% of the students preferred ChatGPT over Gemini (chi-square $\chi^2=6.125$, $p<0.05$) and critical thinking dimension scores ranged from 4.55 for inference to 2.77 for self-regulation. Students refined prompts for an average of 32 times per case. The key limitation of this study is that all data is based on self-reported perceptions. The findings suggest that GenAI tools can accelerate scenario comprehension and enrich educational outcomes.

Keywords: Generative AI (GenAI), MMRIS framework, information security, critical thinking, case study

Recommended Citation: Zhao, G., Tu, C., Adkins, J.K., (2025). Enhancing Student Learning in Information Security Courses: Integrating Generative AI, Critical Thinking, and Case-Based Pedagogy. *Cybersecurity Pedagogy and Practice Journal;* v5(n1) pp 4-16. DOI# https://doi.org/10.62273/STAD3184

Enhancing Student Learning in Information Security Courses: Integrating Generative AI, Critical Thinking, and Case-Based Pedagogy

Gary Yu Zhao, Cindy Zhiling Tu and Joni Adkins

1. INTRODUCTION

Utilizing case studies in an information security class offers numerous pedagogical and practical benefits, especially in boosting student comprehension, engagement, and critical thinking. As established through a comprehensive Delphi Study by the American Philosophical Association (Facione, 1990), critical thinking represents an intentional and self-monitored cognitive process that involves systematically interpreting information, analyzing components, and evaluating both evidence and contextual elements. These skills are essential for the problem-solving mindset. In the context of information security education, students regularly engage in discussions, challenging others' ideas, and approaches to problem-solving (Clarke & Konak, 2025). In a case study, critical thinking involves more than simply analyzing the incident; it requires students to challenge underlying assumptions, assess the validity of evidence, and develop logical, well-reasoned solutions. Throughout this process, students consistently apply analytical thinking and adapt their strategies, thereby demonstrating and strengthening their critical thinking abilities as they work through complex problems (Anderson et al., 2024).

Critical thinking skills and knowledge are generally considered in six dimensions: interpretation, analysis, evaluation, inference, explanation, and self-regulation (Facione, 1990). In the case study of information security, interpretation involves understanding the scenario, defining the problem, and recognizing the stakeholders, systems, and security controls involved. Analysis enables students to analyze the situation, break down the attack chain, examine vulnerabilities, and assess security defenses (Mukherjee et al., 2024). Evaluation involves evaluating evidence, verifying data, and assessing impact and biases (Grover & Pea, 2013). Inference allows students to brainstorm possible solutions, compare alternatives, and predict outcomes (Zimmerman, 2002). Explanation involves decision-making, choosing the best action, and considering ethics and compliance. Finally, self-regulation involves reflecting and improving. This allows students to review mistakes, document lessons learned, and ensure continuous improvement and adaptability (Zimmerman, 2002).

Generative AI (GenAI) technologies like ChatGPT have proven effective in diverse academic fields, performing tasks like encouraging students to question and refine their solutions, creating knowledge-based course content, supporting coding exercises in Java and Python, and offering feedback for learners (Elkhodr & Gide, 2025; Michel-Villarreal et al., 2023). Information security education is especially well-suited for GenAI integration, as it demands both theoretical understanding and hands-on implementation. Students must evaluate regulatory standards, craft security policies, and respond to evolving cyber threats, i.e., tasks that benefit from GenAI-assisted analysis but still necessitate human judgment to ensure precision and applicability (Al-Hawawreh et al., 2023; Balogh et al., 2024; Cao et al., 2025).

The extensive body of literature on GenAI technologies in information security education has documented various advancements; however, several notable gaps persist. Firstly, there is a limited amount of research that specifically investigates the direct impact of GenAI models, such as ChatGPT, on cybersecurity education and curriculum development. Most existing studies have focused broadly on AI, primarily emphasizing earlier technologies like machine learning and data mining (Khan et al., 2024). These studies have explored themes such as personalized learning, adaptive systems, and automated assessments, but they have largely overlooked the distinct capabilities and challenges introduced by GenAI tools. Secondly, there is a paucity of literature addressing how GenAI is integrated with case study pedagogy to promote students' critical thinking and problem-solving skills in the context of information security education. Educators in cybersecurity face the challenge of designing activities that encourage learning through trial and error, while striking the right balance between providing sufficient guidance and fostering independent problem-solving (Ibrahim & Ford, 2023).

This study seeks to bridge these gaps by offering a more in-depth exploration of the educational implications of GenAI, while also analyzing

students' responses and case study developments in the context of these emerging tools. Drawing upon the literature review and the gaps identified in existing research, this work seeks to explore the following research questions:

RQ1: In what ways can GenAI tools be integrated into information security education to strengthen students' critical thinking and their ability to apply knowledge in practical case analysis?

RQ2: How does the use of GenAI tools improve students' critical thinking skills?

By systematically assessing the results of the proposed approach, the study establishes a transferable model for integrating GenAI in the information security curriculum. It serves as a practical reference for educators aiming to leverage AI as a pedagogical tool while maintaining academic rigor and fostering critical thinking.

2. RELATED WORK

Impact of GenAI on Information Security

The transformative capabilities of GenAI—particularly large language models (LLMs) like ChatGPT, image generators, and code synthesis tools, are reshaping the information security landscape, offering innovative solutions for detecting, analyzing, and mitigating security threats (Marquardson, 2024; Shepherd, 2025). Generative AI represents a paradigm shift in both the offensive and defensive dimensions of information security. On the positive side, GenAI enhances threat detection and analysis by enabling systems to recognize complex attack patterns and process large volumes of data more efficiently. It can generate summaries of incidents, analyze logs using natural language understanding, and assist in identifying anomalies that may indicate security breaches (Grover et al., 2023; Metta et al., 2024). Additionally, it supports the automation of defensive measures, such as generating scripts and configurations based on specific threat models, and is being increasingly integrated into Security Orchestration, Automation, and Response (SOAR) platforms to improve response times and accuracy (Metta et al., 2024). GenAI also contributes significantly to cybersecurity training and simulation (Mohawesh et al., 2025). It can create realistic phishing emails, simulated malware, and various attack scenarios, all of which are valuable for red teaming and awareness training without exposing organizations to actual threats. Furthermore, it aids in code and configuration auditing by helping developers identify vulnerabilities in source code or configuration files, often explaining risks in clear, natural language.

Despite these advantages, GenAI introduces a range of security risks. One of the most concerning issues is the automated generation of malware and exploits. Malicious actors can use AI tools to craft polymorphic malware or conceptualize zero-day attacks (Metta et al., 2024). These tools lower the technical barrier for inexperienced attackers, allowing them to generate sophisticated malicious code without advanced expertise. Social engineering and phishing attacks also become more dangerous with the help of GenAI, as it enables the creation of highly personalized, grammatically correct, and context-aware messages, as well as deepfake audio and video content that can convincingly impersonate individuals (Al-Hawawreh et al., 2023).

Data leakage is another significant risk. When organizations interact with AI models—particularly via public APIs—there is potential for inadvertent exposure of sensitive or proprietary information. Furthermore, model inversion attacks may extract confidential data from AI systems that have been trained on private datasets (Okdem & Okdem, 2024). In addition, GenAI can facilitate the evasion of traditional security controls. It can produce obfuscated or encoded malicious content that bypasses intrusion detection systems, firewalls, or other filtering mechanisms, and can adapt dynamically to different environments, undermining static or signature-based defenses (Okdem & Okdem, 2024).

GenAI in Information Security Education

GenAI enhances personalized learning by enabling tailored explanations, real-time tutoring, and adaptive assessments. Students can interact with AI models to clarify difficult concepts such as risk management frameworks, access control models, and compliance requirements (e.g., ISO 27001, NIST, GDPR), receiving instant feedback and examples relevant to their learning pace and context (Bukar et al., 2024; Crabb et al., 2024). Second, GenAI facilitates scenario-based learning and simulations (Elkhodr & Gide, 2025). Instructors can use GenAI to create dynamic case studies, threat models, and incident response simulations that reflect realistic, evolving attack scenarios. These AI-generated exercises can cover a wide range of topics, such as phishing campaigns, insider threats, or ransomware incidents, helping learners practice analytical thinking and decision-making in a safe

environment. Third, GenAI supports content creation and curriculum development (Elkhodr & Gide, 2025). Educators can generate instructional materials, quiz banks, lab exercises, and policy templates efficiently. This not only reduces preparation time but also allows for the rapid updating of content to reflect emerging threats and technologies (Elkhodr & Gide, 2025).

Additionally, GenAI is a useful tool for ethical and critical thinking discussions. It can be used to demonstrate how attackers might misuse AI for malicious purposes, such as generating social engineering scripts or deepfakes, thereby sparking dialogue about responsible AI use, data protection, and legal implications (Mathews et al., 2025).

However, integrating generative AI into information security education also requires caution. There is a risk of students relying too heavily on AI without fully understanding the underlying concepts. Furthermore, the use of GenAI tools must be framed within clear academic integrity policies to prevent misuse, such as plagiarism or unauthorized code generation during assessments (Laato et al., 2020; Michel-Villarreal et al., 2023).

Case Study for Information Security Education

The use of case studies in information security education has become increasingly valuable as a pedagogical tool for bridging theoretical knowledge with practical application (Anderson et al., 2024).

One of the primary benefits of employing case studies is their ability to contextualize abstract security concepts. Topics such as risk assessment, incident response, regulatory compliance, access control, and governance frameworks are often difficult for students to fully grasp through lectures or textbook examples alone (Blanken-Webb et al., 2018; Cai, 2018). Case-based learning situates these concepts in realistic organizational settings, allowing learners to explore how theoretical models apply in practice. Moreover, case studies foster active learning (Cai, 2018; Marquardson, 2024). Instead of passively receiving information, students engage in discussions, analyze evidence, and evaluate alternative strategies. This interaction encourages deeper comprehension and the retention of complex information. For instance, analyzing a case involving a data breach can lead students to consider the interplay between technical controls, user behavior, and management decisions, thereby promoting a holistic understanding of cybersecurity. Case studies also serve to cultivate ethical awareness and policy literacy (García Peñalvo et al., 2025). By examining incidents involving insider threats, compliance failures, or controversial surveillance practices, learners can critically assess legal and ethical dimensions of security decision-making, which is particularly important in a domain where professionals must balance technical effectiveness with privacy rights, legal obligations, and organizational values (Mukherjee et al., 2024; Shivapurkar et al., 2020).

Additionally, case studies support interdisciplinary learning. Information security spans multiple domains— technical, managerial, legal, and behavioral (Mathews et al., 2025; McDonald et al., 2019; Shepherd, 2025). A well-designed case can integrate perspectives from all these areas, encouraging students to synthesize diverse forms of knowledge (Tagarev, 2019). This is particularly useful for graduate-level education or professional development courses, where learners often come from varied backgrounds.

3. METHODOLOGY

This study aims to propose a structured framework for utilizing GenAI tools in information security courses, demonstrating how such technologies can be leveraged to sharpen learners' critical thinking and problem-solving skills. The implementation strategy unfolds in two structured phases. In the first phase, GenAI is incorporated into initial exercises, prompting students to evaluate AI-generated content, assess its validity, and enhance it through independent research and verified sources. This active engagement shifts learning from passive acceptance to critical analysis, reinforcing cybersecurity principles through hands-on scrutiny. The second phase integrates GenAI tools into formal case study assessment, challenging students to adapt AI-produced outputs to real-world cybersecurity situations while refining their work to meet industry and regulatory requirements. To solidify learning, reflective exercises are embedded, requiring students to compare different GenAI tools, evaluate GenAI's role in the case study process, its strengths, and its constraints.

This study was conducted in a graduate-level information security course at a Midwest public university, where one of the primary learning objectives was to prompt students to develop critical thinking and problem-solving skills. This study was built upon a case study in-class

assignment as shown in Appendix A. The assignment required group work, and the total class time was 6 hours over two weeks, with classes on Monday, Wednesday, and Friday (each lasting one hour). The main components of the assignment are summarized below.

No.	Case Title	Case Reference Link
1	ViaSat Attack in Ukraine	https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/ cases/viasat
2	Florida International University Ransomware Attack	https://www.scworld.com/brief/florida-international-university-attacked-by-blackcat-ransomware
3	Rockstar Games Data Breach	https://www.securityweek.com/rockstar-games-confirms-breach-leading-gta-6-leak/
4	A massive DDoS attack takes down Israeli government websites	https://www.timesofisrael.com/government-sites-crash-after-massive-cyberattack-officials-say/
5	Synnovis Healthcare breach in June 2024	https://www.webopedia.com/technology/biggest-cyber-attacks-2024/
6	What Caused the Uber Data Breach in 2022?	https://www.upguard.com/blog/what-caused-the-uber-data-breach
7	South Korea says DPRK hackers stole spy plane technical data	https://www.bleepingcomputer.com/news/security/south-korea-says-dprk-hackers-stole-spy-plane-technical-data/
8	Colonial Pipeline Ransomware Attack	https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
9	Attack on Saudi Aramco	https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html
10	Data of More than 200 Million Twitter Users is Leaked	https://purplesec.us/breach-report/twitter-data-leak-200-million-users/
11	Iranian hackers breached a New York dam in 2013	https://www.ciodive.com/news/iranian-hackers-breached-new-york-dam-in-2013-wsj/411310/
12	Ransomware Breach Disrupted Indonesia Immigration	https://www.sangfor.com/blog/cybersecurity/ransomware-breach-disrupted-indonesia-immigration-and-other-government-services
13	Polycab targeted by ransomware attack	https://www.financialexpress.com/business/industry-polycab-targeted-by-ransomware-attack-company-says-core-systems-and-operations-not-impacted-3432321/
14	WazirX Cryptocurrency Exchange Loses $230 Million in Major Security Breach	https://thehackernews.com/2024/07/wazirx-cryptocurrency-exchange-loses.html

Table 1: The Case Pool for the In-class Assignment

For this in-class assignment, students were required to collaborate in groups to conduct a comprehensive analysis of a historical cyber incident using the Motivation-Methods-Resources-Impact-Solutions (MMRIS) framework adapted from the MMRI model (University of Washington, n.d.).

In phase one (2 class hours), students learned the MMRIS framework and used it to dissect the attack in terms of the attacker's motivation, the methods employed, the resources utilized, the impact of the incident, and the solutions suggested. Then, students practiced prompting two GenAI tools - ChatGPT and Gemini. The prompt must use the MMRIS framework in a cyberattack case. Students could use the 2023 MGM cyberattack case or choose another case. A sample prompt was "Use the MMRIS framework to analyze this cyberattack." Then "What were motivations?" and "What were the methods?" This practice was an iterative process that included a cycle of initializing a prompt, analyzing the output, and refining the prompt. Students kept track of the number of times they refined their prompts.

The second phase (4 class hours) involved randomly drawing and thoroughly reviewing a real-world cyber incident from the case pool (Table 1). The students could describe the attack using their own words or upload the case. Students then applied the MMRIS framework as they had learned in phase one. Again, students must engage with two generative AI tools, such as Gemini and ChatGPT, by prompting them to

analyze the chosen case and compare the resulting outputs. Students all used the free versions of ChatGPT and Gemini. Based on this comparison, each group would develop and present its own analysis using the MMRIS model.

After completing their case analysis, students gave a presentation to their classmates. They then submitted a final reflection, which included the evidence of learning promised in their proposal, as well as insights into their learning experience.

Throughout the assignment, students were encouraged but not limited to use ChatGPT and Gemini in two phases. They could choose Grok, DeepSeek, Claude, or other models. They were instructed to cite ChatGPT and Gemini in both their initial learning plans and final reflections whenever they directly quoted its outputs. The instructor also demonstrated ChatGPT usage in class and provided examples highlighting instances of incorrect responses from the tool.

Once the final reflection was submitted, students were invited to participate in the study, which aimed to inform future classroom discussions. Participation was voluntary, with no course credit or other incentives offered. The study involved completing a single survey featuring both quantitative and qualitative questions. Survey prompts are detailed in the results section. Students also had the option to upload ChatGPT and Gemini chat logs.
No personal identifying information was collected unless a student chose to upload their logs. These logs compromised full anonymity due to filenames containing student names and the uniqueness of each student's topic, which could link the log to an individual.

4. RESULTS

In total, 191 students, divided into 32 groups (six students for 31 groups and five students for the last group), submitted the case study assignment, and all 191 students completed the reflection survey.

In phase one, students reported the count of how many times they refined the prompt based on applying the MMRIS framework (at least five prompts). As shown in Figure 1, the range of refining times is from 15 to 46 for all 32 groups. Group 24 refined the least — 15 times, and Group 19 refined the most — 46 times. The average number of refining times is 32, approximately 6 refinements per query.

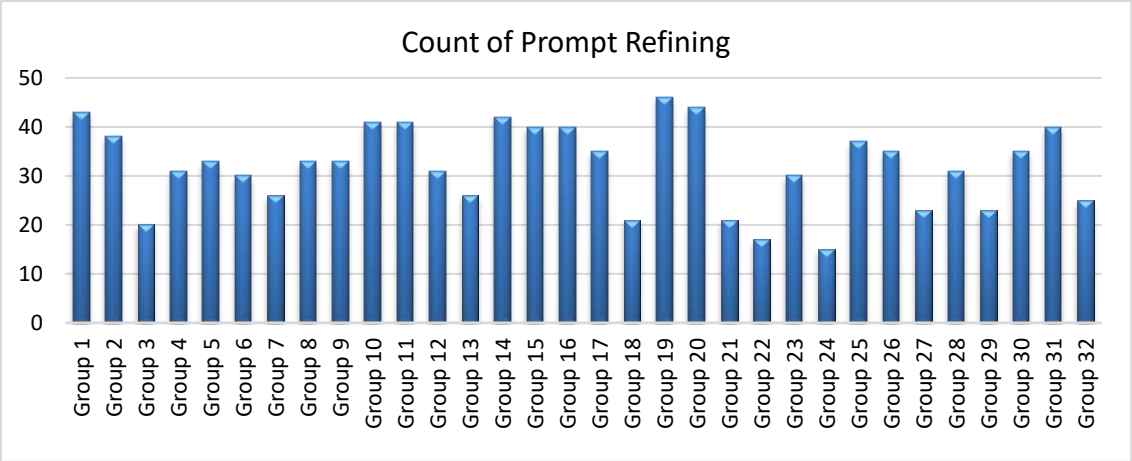


Figure 1. The Count of Prompt Refining

In phase two, students reported comparing their preferences for ChatGPT and Gemini when applying the MMRIS framework to the case study assignment. Figure 2 illustrates the overall group preferences: 72% of groups prefer ChatGPT, while 28% prefer using Gemini (chi-square $\chi^2 = 6.125$, $p < 0.05$, suggesting a clear preference between the two options presented). Moreover, as shown in Figure 3, student groups prefer using ChatGPT versus Gemini on the analysis of attack motivation by a ratio of 18:14, attack methods 16:16, attack resources 22:10, attack impact 17:15, and suggested solutions 21:11. The ANOVA results revealed significant differences among the groups ($F(df1, df2) = 11.701$, $p < 0.05$), and the post-hoc tests identified which specific group comparisons were statistically different.

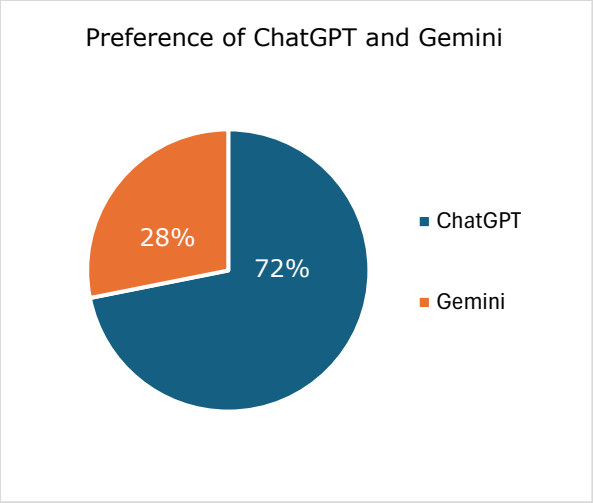


Figure 2. Student Group Preferences of ChatGPT and Gemini

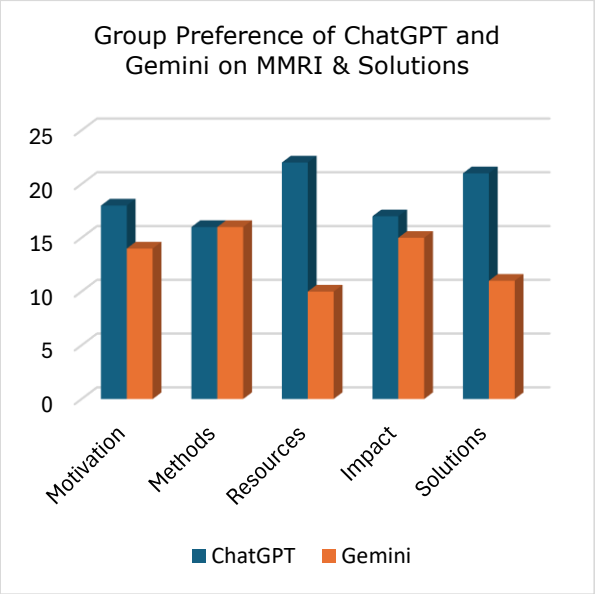


Figure 3. Student Group Preference of ChatGPT and Gemini on MMRI & Solutions

At the end of phase two, a questionnaire survey was completed to gather feedback on the impact of GenAI tools on critical thinking and problem-solving skills. The survey includes 17 questions with a 5-point Likert scale (1=Strongly Disagree, 5=Strongly Agree) covering seven aspects. The survey questions focus on the reflection of six dimensions (Clarke & Konak, 2025) of critical thinking and the intention of using GenAI. A total of 191 feedback responses from students were collected and analyzed. Table 2 shows the survey report.

#	Question	Mean	SD
1	GenAI can learn the MMRIS framework fairly	3.3	0.9
2	GenAI helps me understand the cyber incident scenario and learn the problems	2.9	0.5
3	GenAI helps me recognize the stakeholders, systems, and security controls involved.	3.7	0.6
4	GenAI can help me analyze the attack chain and the situation when an incident occurs.	3.1	0.4
5	GenAI can examine the vulnerabilities in the incident case	4.2	0.5
6	GenAI can help me evaluate the evidence and verify the data provided in the incident case	2.8	0.6
7	GenAI can help me assess the impact on individuals, organizations, and society	3.9	0.4
8	GenAI can suggest possible solutions and predict outcomes	4.6	0.5
9	GenAI helps me consider different perspectives when finding solutions	4.5	1.5
10	GenAI can provide comments on choosing the best action	3.5	1.4
11	GenAI can help me consider ethics and compliance	3.9	1.6
12	GenAI helps me document lessons learned from the incident cases	2.8	1
13	GenAI encourages me to ask deeper or more refined questions	3.1	0.9
14	GenAI helps me identify gaps or overlooked factors in our case study processes	2.4	1.5
15	Overall, GenAI was a valuable tool for enhancing my critical thinking skills	4.1	0.6
16	I would recommend the use of GenAI in future information security case studies or similar assignments	4.7	0.6
17	I have the intention of using GenAI ethically in my future professional practice	4.9	0.7

Table 2. Helpfulness of GenAI on Critical Thinking and Intention of Adoption

As shown in Figure 4, in the six dimensions of critical thinking, students perceived that GenAI tools have a good performance on five dimensions, especially on inference (providing possible solutions, scoring 4.55). The worst

performance is on self-regulation, with a score of 2.77. Additionally, the intention to adopt GenAI is high, with a score of 4.57.

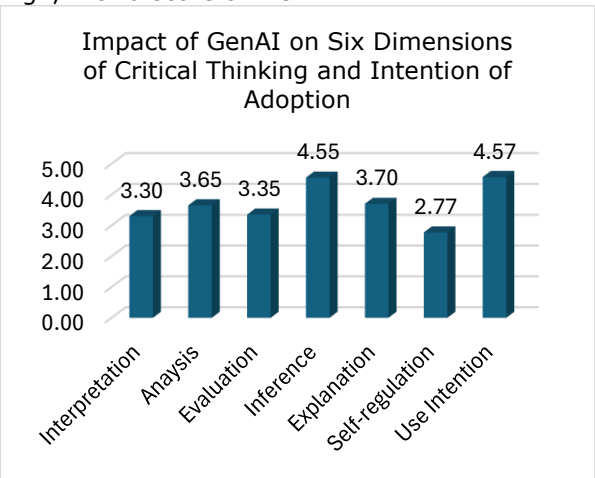


Figure 4. Impact of GenAI on Six Dimensions of Critical Thinking and Intention of Adoption

5. DISCUSSION

Overall, the results suggest that GenAI tools can enhance students' critical thinking skills and support structured analysis using the MMRIS framework in information security case studies; however, despite the high intention to use GenAI tools, students must be aware of potential inaccuracies and ethical issues.

In phase one, students counted the prompt refining times and compared the outputs based on the word changes. All students agreed that refining prompts when using GenAI tools was crucial because the quality of the input (prompt) directly determined the quality of the output (response). However, there is no evidence in our study to show a positive relationship between the refining times and students' satisfaction with the output. It could be a direction for future research.

In phase two, students applied ChatGPT and Gemini with the MMRIS model to case studies and compared the outputs. The results show that students preferred ChatGPT over Gemini with a ratio of 72% to 28%. Additionally, ChatGPT outperformed Gemini in analyzing attack motivation, resources, and impact, as well as in providing possible solutions; however, it tied with Gemini in analyzing attack methods.

"ChatGPT provided a broader perspective, focusing on motivations and methods. Its analysis included high-level recommendations for financial and reputational recovery."

"ChatGPT can be a great tool for generating general information and overviews, especially when needing fast answers on common topics."

"ChatGPT is useful for providing business-focused insights, such as explaining how companies handle crises, respond to threats, and manage operational continuity."

"Our team found ChatGPT to be more user-friendly for broad brainstorming, while Gemini excelled in detailed and actionable insights."

"Gemini suits formal, in-depth needs; ChatGPT offers flexible, quick insights adaptable to follow-up questions."

"Gemini excels in delivering detailed, technical information, especially about the methods and tools used by attackers."

"Gemini offered detailed operational insights and practical steps for mitigating risks. It emphasized post-attack recovery strategies and operational continuity measures."

The above students' feedback affirms the results. ChatGPT is more user-friendly for providing broad and summarized analysis, more efficient for interacting with users' natural language prompts, more effective for engaging the cyber incident contexts, and more concise for organizing related concepts in the responses. Gemini provides more granular, technical breakdowns and organizes responses into detailed subcategories. Moreover, the survey analysis reveals that GenAI significantly enhances the processes of interpretation, analysis, evaluation, inference, and explanation, but performs poorly in self-regulation. Affirmatively, all students agree that both ChatGPT and Gemini help users develop critical thinking and problem-solving skills.

Based on the analysis and discussion of the survey and students' feedback, we propose a conceptual framework that integrates GenAI tools, critical thinking, and the MMRIS framework to support the analysis of cybersecurity case studies.

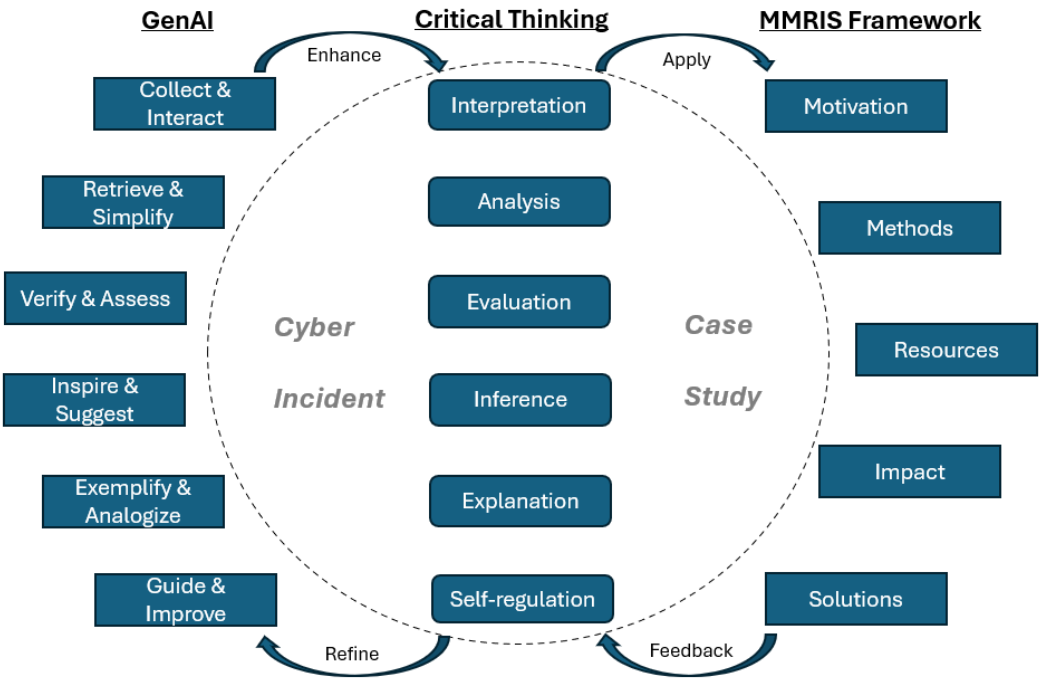


Figure 5. A Conceptual Framework

As shown in Figure 5, at the center of the diagram is the case of a cyber incident, which serves as the focal point for applying both technological and cognitive tools in an educational context. On the left side of the diagram, GenAI tools, such as ChatGPT, Gemini, or similar models, play a supporting role by offering a variety of cognitive and assistive functions. These tools enable users to collect and interact with information, retrieve and simplify complex data, verify the credibility of sources, generate suggestions, provide examples and analogies, and guide users toward continuous improvement. These functionalities contribute to enhancing and refining students' critical thinking processes throughout the case analysis. Critical thinking itself is situated at the core of the framework, depicted as a sequence of interconnected cognitive activities. These include interpretation, analysis, evaluation, inference, explanation, and self-regulation. These thinking processes are not isolated; they are supported and enriched by GenAI's capabilities, which offer feedback and opportunities for iterative improvement. On the right side of the diagram lies the MMRIS framework, comprising motivation, methods, resources, impact, and solutions, which provides a structured approach to dissecting and understanding the selected cybersecurity incident. Through the application of critical thinking skills, students are encouraged to examine why the incident occurred, how it was executed, what tools were involved, what effects it had, and how the situation was or could be resolved.

The framework also highlights the dynamic interaction between these components. GenAI tools enhance critical thinking, which in turn supports the application of the MMRIS framework to the case study. The process includes a feedback loop where self-regulation, supported by AI guidance, leads to refined analysis and deeper learning. Overall, the framework emphasizes how the integration of GenAI, structured analytical models, and critical thinking skills can significantly enrich students' ability to interpret, evaluate, and respond to real-world cybersecurity challenges.

6. CONCLUSIONS

This study sheds light on how GenAI tools can be utilized to enhance learning in the field of information security. We propose a structured framework for incorporating GenAI into cybersecurity education, highlighting its ability to improve critical thinking and hands-on problem-solving skills. The framework illustrates a pedagogical model for teaching cybersecurity through case-based learning. It emphasizes how GenAI tools, when integrated with critical thinking skills and a structured analytical framework (MMRIS), can enhance students' abilities to understand and respond to complex cyber

incidents. This approach provided students with immersive, practical experience in AI-driven cybersecurity strategies.

Using a case-study-centered pedagogical approach, the study illustrates how GenAI can enhance students' critical thinking in six dimensions. The findings reveal that GenAI significantly accelerates understanding of the scenarios, allowing students to dedicate more time to evaluating, refining, and ensuring compliance with industry standards and regulations. The proposed case analysis method supported by GenAI can be adapted to disciplines beyond security education, reinforcing the generalizability of the pedagogical model.

This study has several limitations that warrant consideration. First, the findings are based on a single academic term and a relatively small student group. Thus, the effectiveness of the proposed framework may vary across different information security curricula and different institutions. Second, the study did not set a control group to compare with and without GenAI integration across different sections or semesters. Third, the research did not objectively assess students' ability to identify inaccuracies in AI-generated content. Future studies should address this gap by examining how detection capabilities vary between novice and advanced learners, thereby exploring potential correlations between skill level and discernment of AI-generated misinformation. Further, future research should investigate the long-term effects on student skill development, adaptive GenAI-learning frameworks, and scalable methods for integrating GenAI into cybersecurity education programs.

7. REFERENCES

Al-Hawawreh, M., Aljuhani, A., & Jararweh, Y. (2023). Chatgpt for cybersecurity: Practical applications, challenges, and future directions. *Cluster Computing*, *26*(6), 3421–3436. https://doi.org/10.1007/s10586-023-04124-5

Anderson, A., Ahmad, A., & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. *Information & Management*, *61*(7), 104015. https://doi.org/10.1016/j.im.2024.104015

Balogh, Š., Mlynček, M., Vraňák, O., & Zajac, P. (2024). Using Generative AI Models to Support Cybersecurity Analysts. *Electronics*, *13*(23), 4718. https://doi.org/10.3390/electronics13234718

Blanken-Webb, J., Palmer, I., Deshaies, S.-E., Burbules, N. C., Campbell, R. H., & Bashir, M. (2018). *A Case Study-based Cybersecurity Ethics Curriculum*. 2018 USENIX Workshop on Advances in Security Education (ASE 18). https://www.usenix.org/conference/ase18/presentation/blanken-webb

Bukar, U. A., Sayeed, Md. S., Fatimah Abdul Razak, S., Yogarayan, S., & Sneesl, R. (2024). Decision-Making Framework for the Utilization of Generative Artificial Intelligence in Education: A Case Study of ChatGPT. *IEEE Access*, *12*, 95368–95389. https://doi.org/10.1109/ACCESS.2024.3425172

Cai, Y. (2018). Using Case Studies To Teach Cybersecurity Courses. *Journal of Cybersecurity Education, Research and Practice*, *2018*(2). https://doi.org/10.62915/2472-2707.1041

Xiao, H., Shah, B., Spring, J., Kuzminykh, I., & Janku, S. (2025). Scaffolding Student Learning through GenAI in Cybersecurity Education. In *The 3rd International Workshop on Cyber Security Education for Industry and Academia (CSE4IA 2025), Munich, Germany*.

Clarke, C. J. S. F., & Konak, A. (2025). The Impact of AI Use in Programming Courses on Critical Thinking Skills. *Journal of Cybersecurity Education, Research and Practice*, *2025*(1). https://doi.org/10.62915/2472-2707.1220

Crabb, J., Hundhausen, C., & Gebremedhin, A. (2024). A Critical Review of Cybersecurity Education in the United States. *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1*, 241–247. https://doi.org/10.1145/3626252.3630757

Elkhodr, M., & Gide, E. (2025). *Integrating Generative AI in Cybersecurity Education: Case Study Insights on Pedagogical Strategies, Critical Thinking, and Responsible AI Use* (arXiv:2502.15357). arXiv. https://doi.org/10.48550/arXiv.2502.15357

Facione, P. A. (1990). *Critical Thinking: A Statement of Expert Consensus for Purposes of Educational Assessment and Instruction.*

Research Findings and Recommendations. https://eric.ed.gov/?id=ED315423

García Peñalvo, F. J., Casany Guerrero, M. J., Alier Forment, M., & Pereira Varela, J. A. (2025). The ethics of generative artificial intelligence in education under debate. A perspective from the development of a theoretical-practical case study. *Revista Española de Pedagogia, 83*(291).

https://doi.org/10.22550/2174-0909.4132

Grover, S., Broll, B., & Babb, D. (2023). Cybersecurity Education in the Age of AI: Integrating AI Learning into Cybersecurity High School Curricula. *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1*, 980–986. https://doi.org/10.1145/3545945.3569750

Grover, S., & Pea, R. (2013). Computational thinking in K–12: A review of the state of the field. *Educational Researcher*, *42*(1), 38–43. https://doi.org/10.3102/0013189X12463051

Khan, M. I., Arif, A., & Khan, A. R. A. (2024) The Most Recent Advances and Uses of AI in Cybersecurity. Jurnal Multidisiplin Ilmu, vol. 3, no. 4, 2024, pp. 566-578.

Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A., & Airola, A. (2020). AI in Cybersecurity Education- A Systematic Literature Review of Studies on Cybersecurity MOOCs. *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)*, 6–10. https://doi.org/10.1109/ICALT49669.2020.00009

Marquardson, J. (2024). Embracing Artificial Intelligence to Improve Self-Directed Learning: A Cybersecurity Classroom Study. *Information Systems Education Journal*, *22*(1), 4–13.

Mathews, N., Schwartz, C., & Wright, M. (2025). Teaching Generative AI for Cybersecurity: A Project-Based Learning Approach. *Journal of The Colloquium for Information Systems Security Education*, *12*(1), Article 1. https://doi.org/10.53735/cisse.v12i1.211

Mcdonald, J., Hansen, D., Balzotti, J., Tanner, J., Winters, D., Giboney, J., & Bonsignore, E. (2019). *Designing Authentic Cybersecurity Learning Experiences: Lessons from the Cybermatics Playable Case Study*. http://hdl.handle.net/10125/59689

Metta, S., Chang, I., Parker, J., Roman, M. P., & Ehuan, A. F. (2024). *Generative AI in Cybersecurity* (arXiv:2405.01674). arXiv. https://doi.org/10.48550/arXiv.2405.01674

Michel-Villarreal, R., Vilalta-Perdomo, E., Salinas-Navarro, D. E., Thierry-Aguilera, R., & Gerardou, F. S. (2023). Challenges and Opportunities of Generative AI for Higher Education as Explained by ChatGPT. *Education Sciences*, *13*(9), Article 9. https://doi.org/10.3390/educsci13090856

Mohawesh, R., Ottom, M. A., & Salameh, H. B. (2025). A data-driven risk assessment of cybersecurity challenges posed by generative AI. *Decision Analytics Journal*, *15*, 100580. https://doi.org/10.1016/j.dajour.2025.100580

Mukherjee, M., Le, N. T., Chow, Y.-W., & Susilo, W. (2024). Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information*, *15*(2), Article 2. https://doi.org/10.3390/info15020117

Okdem, S., & Okdem, S. (2024). Artificial Intelligence in Cybersecurity: A Review and a Case Study. *Applied Sciences*, *14*(22), Article 22. https://doi.org/10.3390/app142210487

Shepherd, C. (2025). *Generative AI Misuse Potential in Cyber Security Education: A Case Study of a UK Degree Program* (arXiv:2501.12883). arXiv. https://doi.org/10.48550/arXiv.2501.12883

Shivapurkar, M., Bhatia, S., & Ahmed, I. (2020). Problem-based Learning for Cybersecurity Education. *Journal of The Colloquium for Information Systems Security Education*, *7*(1), Article 1.

Tagarev, N. (2019). *Role of Case Study Analyses in Education of Cybersecurity Management*. Proceedings of the 13th International Multi-Conference on Society, Cybernetics and Informatics (IMSCI 2019), pp.61-64.

University of Washington. (n.d.). *The Security Cards: A Security Threat Brainstorming Kit*. Retrieved June 7, 2025, from https://securitycards.cs.washington.edu/

Zimmerman, B. J. (2002). Becoming a Self-Regulated Learner: An Overview. *Theory Into Practice*, *41*(2), 64–70. https://doi.org/10.1207/s15430421tip41022

APPENDIX A

The Group Assignment of Case Study with GenAI

In this class work, you need to work with your group members to complete the following tasks:

1. Go through a case of a cyber incident that occurred in the past.
2. Learn and apply the Motivation-Methods-Resources-Impact-Solutions (MMRIS) framework to the cyber incident case.

   MMRIS materials are linked under Module 12 on the course site.
3. Prompt two generative AI tools (Gemini, ChatGPT, Grok, Claude, etc.) using MMRIS and present the outputs.
4. Compare the output difference between two AI tools.
5. Propose your own analysis based on MMRIS.
6. Address what you have learned about using Gen-AI tools for this case study.

At the end of Monday's class, you must submit at least 15 PowerPoint slides covering the above topics.

You will do a class presentation on Wednesday and Friday's classes.

Here is the rubric:

44652 - Group Case Study Presentation Scoring Guide Section No:					
Group Names (First name Last name)	M1:		M4:		
	M2:		M5:		
	M3:		M6:		
Group Asssesment	Case Title:		Total Points	Points Awarded	
	1) Title slide contains team name and team members, total >12 slides		1		
	2) Case Introduction		2		
	3) ChatGPT prompt and answers(motivation, methods, resources, impact)		4		
	4) Gemini prompt and answers (motivation, methods, resources, impact)		4		
	5) Comparison on two generative AI answers, differences?		4		
	6) What are your own analysis based on these AI tools (motivation, methods, resources, impact)?		5		
	7) What have you learned on how to use these AI tools?		5		
	Total		25		

		Total Points	M1	M2	M3	M4	M5	M6
Individual Assessment	Member time limits >1 minute	4						
	Team total time 8-10 minutes	2						
	Effective use of notes (note cards or paper notes)	4						
	Professionalism (appropriate gestures, posture, professional attire)	4						
	Eye contact	2						
	Voice control (pitch, rate, volume)	2						
	Appropriate pace of speech, interaction	2						
	Total	20	0	0	0	0	0	0

Excessive Equating: An Exploration of Knowledge Unit (KU) Curricular Load for CAE-CD Program Design and Evaluation

Kasey Miller
millerkc@uncw.edu

Kevin Matthews
matthewskd@uncw.edu

Ulku Clark
clarku@uncw.edu

Geoff Stoker
stokerg@uncw.edu

Congdon School
University of North Carolina Wilmington
Wilmington, NC 28403 USA

Abstract

The growing demand for rigorous, standardized cybersecurity education has made the NSA's National Centers of Academic Excellence in Cybersecurity (NCAE-C) program a cornerstone in ensuring quality and consistency across institutions. The NCAE-C program for Cyber Defense utilizes the fundamental element Knowledge Unit (KU) to bundle learning outcomes and topics. Institutions designated a Center of Academic Excellence (CAE) under the NCAE-C program must validate at least one program of study (PoS) by mapping PoS courses to a specified number and set of KUs. This ensures that the CAE's PoS includes foundational cybersecurity content and provides sufficient breadth and depth. A simplifying NCAE-C program guideline treats all KUs as equivalent for mapping and validation purposes, regardless of the number or difficulty of learning outcomes and topics. In this paper, we suggest that a more granular approach may be appropriate when comparing KUs. Using systematic counts of learning outcomes and topics, combined with Bloom's Taxonomy weighting of cognitive verbs, we calculate curricular load scores for all 73 KUs in the CAE-CD program. These findings suggest that uniform treatment of KUs may unintentionally introduce inequities into CAE-CD program design, review, and evaluation. Recommendations include standardizing verb usage across KU documents and considering KU complexity when developing or revising program criteria. A more granular understanding of KU demands can enhance curriculum planning and strengthen both academic rigor and alignment with evolving cybersecurity needs.

Keywords: Knowledge Unit (KU), CAE-CD, Bloom, Cybersecurity Pedagogy

Recommended Citation: Miller, K., Matthews, K., Clark, U.Y., Stoker, G., (2025). Excessive Equating: An Exploration of Knowledge Unit (KU) Curricular Load for CAE-CD Program Design and Evaluation. *Cybersecurity Pedagogy and Practice Journal;* v5(1) pp 17-40. DOI# https://doi.org/10.62273/SYPT8785

Excessive Equating: An Exploration of Knowledge Unit (KU) Curricular Load for CAE-CD Program Design and Evaluation

Kasey Miller, Kevin Matthews, Ulku Clark, Geoff Stoker

1. INTRODUCTION

One of the two main requirements for designation in the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program for Cyber Defense (CD) is a validated Program of Study (PoS) (Application Process and Adjudication Rubric Cyber Defense Working Group, 2024). A major part of validating a PoS for a bachelor's program involves aligning 22 knowledge units (KU) with relevant courses within the PoS [NOTE: KU alignment details differ across associate, master's, and doctoral programs]. "A Knowledge Unit (KU) is a thematic grouping that encompass [*sic*] multiple, related KU outcomes and learning topics." (Application Process and Adjudication Rubric Cyber Defense Working Group, 2024, p. 3). In this paper, the term "curricular load" refers to an abstract measure of the academic burden associated with a set of learning outcomes and topics. Although this concept is explained more fully later, for now, think of curricular load as the idea that covering one learning outcome is less demanding than covering two, and addressing one topic is less burdensome than addressing two.

Currently, there are 73 KUs grouped as follows:

- 3 Foundational KUs
- 5 Technical Core KUs
- 5 Non-technical Core KUs
- 60 Optional KUs.

Each validated PoS in a bachelor's degree program must align with 1) the 3 Foundational KUs, 2) *either* all 5 Technical Core KUs *or* all 5 Non-technical Core KUs, and 3) 14 of the Optional KUs (*NOTE: opposing core KUs may also be used as optional KUs – i.e., if the Technical Core is chosen, then Non-technical Core KUs may be used as optional KUs, and vice versa*). Each KU contains a list of learning outcomes and a list of topics. "While it is not required that every learning outcome be explicitly assessed as written, applicant schools should be able to defend their coverage of the learning outcomes" (Becker et al, 2024, p. 3). For KU topics coverage, a simple majority must be addressed.

The NCAE-C Program for CD instruction document also specifies that "a KU may be covered by one or more courses; however, a course should not be aligned to an excessive number of KUs, given the challenge of so many KU Outcomes coverage with a single course" (Becker et al, 2024, p. 3). The meaning of *excessive* is not clarified in this document, but in recent guidance from the NCAE-C program office, the number five has been suggested as the threshold above which mapped KUs to a single course would be scrutinized (S. Steiner, personal communication, May 22, 2025).

While this guidance begins to clarify what excessive could mean and is administratively useful, it is a bit coarse-grained and seems to imply, likely unintentionally, that the curricular load of all KUs is equivalent, so 1 KU ≡ 1 KU, despite the variation in the number of learning outcomes and topics for each KU. Among the 73 KUs, the number of learning outcomes per KU ranges from 1 to 10, and the number of topics ranges from 5 to 41. At the extremes, the KU Software Security Analysis (SSA) has 2 Learning Outcomes and 5 Topics, whereas the KU Hardware/Firmware Security (HFS) has 5 Learning Outcomes and enumerates 41 Topics.

Although CAE CD policy treats all KUs as equivalent, the number of learning outcomes, topics, and Bloom-level verbs varies dramatically. Without accounting for this variation, KU mapping may unintentionally penalize programs whose selected KUs carry disproportionately high cognitive or topical load.

This observation raises some questions, the exploration of which seems likely to be beneficial to the CAE-CD community. Specifically, what is a good way to assess the curricular load of a particular KU? Would having a curricular load score for each KU be helpful when evaluating a school's PoS? Would a curricular load score help schools interested in applying to the NCAE-C program better align KUs to their curriculum?

In this paper, two ideas for generating a KU curricular load score using the number of KU Learning Outcomes, the number of KU Topics, and the revised Bloom's Taxonomy level associated with the measurable verbs in the KU Learning Outcomes are explored. Section 2 reviews Bloom's Taxonomy very lists and prior KU

analysis to motivate why verb choice matters for curricular burden. Section 3 details two scoring techniques, unweighted curricular load score (UCLS) and weighted curricular load score (WCLS), and the coding protocol used. Section 4 reports the results across KUs and illustrates the differences between UCLS and WCLS. Section 5 interprets the results for academic units from course design and program evaluation perspectives. Section 6 concludes with implications for standards-aligned curricula beyond CAE-CD.

2. LITERATURE REVIEW

In 1948, an informal meeting of college examiners sparked interest in creating a theoretical framework to facilitate communication and the exchange of assessment items across educational institutions that measure common educational objectives (Bloom et al., 1956; Krathwohl, 2002). The original idea included plans for a taxonomy of three domains: *cognitive*, *affective*, and *psychomotor*. After years of work, a handbook was published on the cognitive domain, focusing on "the recall or recognition of knowledge and the development of intellectual abilities and skills" (Bloom et al., 1956, p. 7). The six major classes identified were: *knowledge*, *comprehension*, *application*, *analysis*, *synthesis*, and *evaluation*.

About half a century later, the framework was revised by a group that included David R. Karthwohl, a key contributor and author of the original framework, and resulted in the renaming of three classes, the reordering of two, and the recasting of all to verb form: *remember*, *understand*, *apply*, *analyze*, *evaluate*, and *create* (Krathwohl, 2002).

Verbs

Using the presence of specific verbs in learning objectives to help identify and map objectives to Bloom levels has been done since the 1956 publication of the original taxonomy; however, an authoritative, non-level-overlapping list of verbs does not currently exist. Several efforts have been made to curate such a list, and we explore here the five that we consulted.

Thirty unique verb lists were gathered by Stanny (2016) from the top 30 results of a Google search for "action words for Bloom's taxonomy" (Stanny, 2016, p. 3). From this collection of 788 verbs, she found 433 unique verbs and 355 duplicates, both within and across the six Bloom categories. Using frequency of appearance across the 30 lists, Stanny created a list of 104 unique verbs that each appeared on 10 or more lists. These 104 verbs resulted in a 128-verb chart with 18 words duplicated across Bloom categories and the triplication of three (Figure A-1).

Newton et al. (2020) gathered 47 publicly available lists from 35 universities and textbooks, noting that there was "very little agreement between these lists, most of which were not supported by evidence explaining where the verbs came from" (Newton et al., 2020, p. 1). Across the lists, they found 401 unique verbs. They created a 51-verb list with no duplicates using the original Bloom categories. It included only verbs that appeared on more than half of the lists, occurring 50% of the time in one category (Figure A-2).

In 2022, Das et al. built upon Stanny's work and created a four-level classification system: Level 1, unambiguous; Level 2, unambiguous with a lower threshold; Level 3, transitional verbs; and Level 4, ambiguous. Level 1 results in 83 verbs, which is Stanny's 128-verb chart minus the 21 verbs that repeat (Figure A-3).

In January 2023, the Association for Computing Machinery (ACM) Committee for Computing Education in Community Colleges (CCECC) published a report that included a chart with 142 unique verbs (Bamkole et al, 2023). While many of the verbs are common to lists found on the internet, the main purpose of the report was to curate verbs useful to the computing community and for "technical tasks for which a technical verb would be appropriate but is not available" (Bamkole, 2023, p. 5). For example, they took the verbs *code*, *script*, and *program*, which indicate similar concepts, and assigned *code* to the Apply level and *script* and *program* to the Create level. The published list includes 56 of these compute-related verbs (Figure A-4).

For their 2024 article, ElJishi et al. obtained lists of action verbs aligned to the revised Bloom's Taxonomy from Stanford, Harvard, and an open textbook by Zhou & Brown (2015). They used consensus to avoid duplicating verbs across Bloom categories and created a 140-verb list, albeit with 4 duplicates (Figure A-5).

KU Analysis

Previous analysis evaluated the 2018-2019 changes to KU mapping and the reorganization of KU groups from two-year core, four-year core, and optional to the current groups of foundational, technical core, non-technical core, and optional (Clark et al., 2020). This paper considers the KUs with changes published in late

2024 and focuses on their learning objectives and topics.

3. METHODOLOGY

Curricular load scores for each of the 73 KUs were generated in two ways: an unweighted method and a weighted method incorporating the revised Bloom's taxonomy levels. A complicating factor for both methods was how to count topics in the 36 KUs with enumerated subtopics. In these cases, only subtopics were counted, and the topic was treated as a heading. In Figure 1, for example, the Technical Core KU Basic Scripting and Programming (BSP) has eight numbered topics, one of which (number 8) includes 10 subtopics enumerated by lowercase letters a. through j. In this case, we count 17 topics for the BSP KU (7 topics + 10 subtopics).

Topics

1. Basic security concepts
2. Permissions (e.g., Linux, Windows, MacOS), bounds checking, input validation, type checking and parameter validation
3. Fundamental concepts and basic implementation of regular expressions
4. Fundamental data structures and algorithms
5. Boolean logic/operations (e.g., AND / OR / XOR / NOT)
6. Scripting language on both Windows and Linux (e.g. PERL, Python, BASH, JAVA, VB Scripting, Powershell)
7. Integrated Development Environment (IDE), Compilers/Interpreters
8. Properly apply basic programming constructs and concepts including:
    a. Variables and types (e.g., int, float, char, etc.)
    b. Strings, arrays, structures
    c. Sequential and parallel execution
    d. Assignments (e.g., :=, =, ++, --, etc.)
    e. Decisions and branching (e.g., if, if ... else, elseif, switch, case, etc.)
    f. Loops (e.g., for, while, repeat, etc.)
    g. Functions, procedures, and calls
    h. Debugging techniques
    i. Console and file I/O
    j. Libraries

Figure 1: BSP KU topics count = 17 – topics 1-7 plus subtopics 8.a.-8.j. (Becker et al., 2024, p. 20).

For Information Assurance Compliance (IAC), this one KU with sub-subtopics (Becker et al., 2024, p. 73) followed the same guideline. In this case, only the sub-subtopics were counted; the topic and subtopic were treated as headings.

Unweighted Curricular Load Scores

The unweighted curricular load score (UCLS) is simply a count of the enumerated learning outcomes and listed topics for each KU. For example, the KU Systems Certification and Accreditation (SCA) has 2 numbered learning outcomes and 5 numbered topics (Figure 2), so the UCLS for SCA is 7 (i.e., 2 + 5).

Weighted Curricular Load Scores

The weighted curricular load score (WCLS) calculation involves an additional step: weighting each learning outcome. Instead of a value of 1, as with UCLS, each learning outcome is given a value (weight) from 1 to 6 based on the Bloom's Taxonomy category into which the verb maps. The SCA KU (Figure 2) learning outcome #1 verb, *describe*, maps to Bloom's *understand* tier (level 2), and the learning outcome #2 verb, *define*, maps to Bloom's *remember* tier (level 1). The weighted score for the SCA KU topics is 2 + 1 = 3, and the WCLS is 8 (3 weighted topic score + 5 topics).

KU Learning Outcomes

To complete this KU, students will be able to:

1. Describe the DoD system certification and accreditation processes.
2. Define certification and accreditation.

Topics

1. DoD Policies and Directives
2. Roles/Players
3. Components of the C&A Process
4. Certification Boards and Panels
5. NIST Risk Management Framework (SP800-37)

Figure 2: Learning Outcomes and Topics for the SCA KU.

For learning outcomes with a single verb, the mapping is straightforward. For learning outcomes with more than one verb, we map it to the Bloom level of the highest-order verb. For example, learning outcome #2 for the Optional KU Data Administration (DBA) reads: "Define and evaluate data and information quality, accessibility, and utility" (Becker et al, 2024, p. 53). This learning outcome has two action verbs: *define* and *evaluate*. Define maps to Bloom's *remember* tier (level 1) and evaluate maps to the *evaluate* tier (level 5), so this learning outcome would have a weight of five.

Results for all UCLS and WCLS values for each KU are provided in detail in Tables B-2 and B-3 and depicted graphically in Figures B-1 through B-3.

Counting and Coding

To identify potential errors or omissions in reviewing the KUs, three authors independently reviewed the KU document, focusing on each of the 73 KUs' learning outcomes and topics. A spreadsheet that captured three things for each KU was produced by each author:

- count of the learning outcomes
- count of the topics
- verb(s) in each learning outcome

After all 73 KUs were coded by each author, the results were compared. All three coders met to review discrepancies and unanimously agreed on the correct code for each disagreement.

First, the codes for the count of learning outcomes were reviewed, and one KU showed a

disagreement (0.014%). Upon further review, one coder mistakenly swapped the values for the learning outcome and topic counts for this KU.

Next, the codes for topic counts were reviewed, and disagreements were identified in 14 KUs (19.178%). Upon further review, there were two main categories of coding disagreements: formatting issues in the Becker et al. (2024) document and human error during the coding process. Only one disagreement fell outside these categories and could not be explained. Nevertheless, all disagreements were easily resolved with unanimous agreement among all three coders.

The formatting issues in the Becker et al. (2024) document accounted for 6 disagreements and can be broken down into 3 types. Four disagreements occurred because a page break separated the enumerated topics, and one coder missed the orphaned topics on the following page (e.g., p. 10). One disagreement occurred because the KU topics list was missing a line break, and the final topic was included on the same line as the previous subtopic (p. 73). The final disagreement was over the inclusion of three "examples of acceptable operating system specific Topics" for the Host Forensics (HOF) KU (p. 71). These operating system-specific examples were ultimately determined to be extensions of previous topics that were already counted in that KU. While this is not necessarily a "formatting" issue with the document, it was the only KU that had such a supplemental list.

Human errors led to seven coding disagreements and can be broken down into four types. One disagreement, paired with the learning outcome disagreement, where the coder swapped the counts of the learning outcomes and the topics. Three disagreements occurred because one or more coders did not include subtopics in a KU's topic count. Two disagreements occurred due to typos: a coder prepended a 1 to the count (i.e., 19 instead of 9 and 15 instead of 5). And finally, one disagreement occurred because a coder mistakenly coded a KU in the wrong row of the spreadsheet; that is, they coded the previous KU instead of the current KU. These types of errors were located, resolved, and support our decision to have multiple coders.

The final thing to review was the verb(s) in each learning outcome. For all 73 KUs, there were 293 learning objectives. Of these 293 learning objectives, 94 (32.082%) contained more than 1 action verb and required a decision of which verb had the highest Bloom level. After all coding was completed, there were disagreements with 36 of the 293 verbs selected (12.287%).

Disagreement over verbs required a bit more discussion among the coders than did the counts of learning outcomes and topics. Once disagreements were identified, all three coders reviewed discrepancies together, adjusted the verb selection process as needed, and unanimously agreed on the selected verb. The reconciliation process revealed a few trends in the discrepancies. These trends were all rooted in the interpretation of the learning objectives and in the ability to reliably reach the same conclusion for a selected verb. In its simplest form, the disagreement was over the order of the listed verbs. For example, if a learning objective contained two verbs at the same Bloom level, sometimes the coders selected the verb that occurred first in the sentence, while other times they selected the alphabetically ranked verb. For consistency, the verb written first in the learning objective was selected.

Surprisingly, the verb selection process also involved parsing the learning objective to identify verb candidates and ruling out verbs that were merely supplemental to the learning objective's action. For example, learning objective #2 for Basic Networking (BNW) reads, "Apply networking concepts to design a basic network architecture given a specific need and set of hosts/clients" (Becker et al., 2024, p. 18). While all coders identified "apply" as an action verb, they differed in how they treated the word "design." After discussion, it was agreed that "to design" was supplemental to the primary action verb "apply" and that this and any subsequent constructions of "to [verb]" would be treated similarly. The same rule was also applied to a sentence with the construction "to [verb1] and [verb2]", reading "verb2" as having an implied "to" just before it. For example, Media Forensics (MEF), learning objective #2 reads, "Apply forensics techniques to investigate and [to] analyze a particular media in context" (Becker et al., 2024, p. 84).

Another interesting discrepancy arose with learning objective #2 for the Optional KU Network Forensics (NWF), which reads, "Analyze and decipher network traffic, identify anomalous or malicious activity, and provide a summary of the effects on the system" (Becker et al., 2024, p. 86). In this case, one author coded "provide a summary" as "summarize" instead of "provide." Though there was general agreement that "summarize" was probably a better verb for that learning objective, coding was restricted to the

document's original text only.

Mapped Verbs

When determining which verbs map to which Bloom levels, the study relied heavily on previous efforts to curate consensus lists (Bamkole et al., 2023; Das et al., 2022; ElJishi et al., 2024; Newton et al., 2020; Stanny, 2016). Each unique verb from the KUs was placed into a Bloom category by referencing the lists in Figures A-2 through A-5. If the verb was in the same category in all 4 lists, placement was easy. If a verb was missing in one or more lists, and the remaining lists had the verb in the same category, placement was also easy. For conflicting listings, we developed the following rules to help us place verbs:

- If 3 of 4 or 2 of 3 lists agreed, the majority ruled
- If 1-1 or 2-2 tie, default to the ACM list
- If 1-1 tie with no ACM or no list had the verb, the verb was placed using the researchers' judgment

The final verb list and Bloom-level categorizations are shown in Table 1. Of the 70 unique verbs across all 73 KUs' learning outcomes, complete consensus mapping was found for 14 (20%) of the verbs (***bold/italics*** Table 1) and some degree of consensus for an additional 20. A single source was used to map 16 verbs. For 20 verbs, categorization was based on the researchers' judgment because none of the lists contained those verbs, or there was conflicting Bloom-level alignment across two lists that were not the ACM list. The details of the placement results are reflected in Table B-1.

Unweighted Technique

Using the unweighted method, it is found that the Systems Certification and Accreditation (SCA) KU was the most lightweight with a UCLS of 7 (2 learning outcomes + 5 topics), and the Hardware/Firmware Security (HFS) KU was the most heavyweight with a UCLS of 46 (5 learning outcomes + 41 topics). A list of all KUs ordered by UCLS is provided in Table B-2.

Weighted Technique

Using the weighted method, it is found that the Systems Certification and Accreditation (SCA) KU was still the most lightweight with a WCLS of 8 – 2 learning outcomes: (1 * level 1 + 1 * level 2 = 3) + 5 topics – while the Intrusion Detection/Prevention Systems (IDS) KU became the most heavyweight with a WCLS of 55 – 7 learning outcomes: (5 * level 3 + 1 * level 4 + 1 * level 5 = 24) + 31 topics. A list of all KUs ordered by WCLS is provided in Table B-3. A list of all KUs, ordered by verb weight, with the corresponding learning outcome verbs used for the weighting process when calculating the WCLS, is provided in Table B-4. A list of the 94 multiple-verb KU learning outcomes is provided in Table B-5, with the verbs not used in the weighting calculation identified.

Remember
define, identify, ***list***, ***recall***, recognize, select
Understand
annotate, communicate, describe, ***discuss***, ***explain***, explore, review, understand
Apply
apply, assist, compute, conduct, configure, demonstrate, deploy, document, draw, execute, handle, harden, illustrate, implement, install, leverage, map, mitigate, perform, produce, protect, provide, quantify, ***use***, utilize
Analyze
analyze, articulate, categorize, characterize, compare, ***contrast***, decipher, detect, diagram, differentiate, examine, monitor, outline, resolve
Evaluate
assess, determine, ***evaluate***, rate, recommend, set up, suggest, test
Create
create, ***design***, develop, devise, organize, ***plan***, propose, prototype, write

Table 1: 70 unique verbs across the 73 KUs mapped to the Revised Bloom's Taxonomy. Verbs in bold indicate complete consensus for mapping across all source verb lists.

4. RESULTS

Verbs

From the 402 measurable verbs used across the 73 KUs' 293 learning outcomes, 70 unique verbs were found. The verb *describe* was used 91 times (22.6% of the 402). There were 34 verbs used a single time (Table 2), for a total of 8.5% of the 402 verb uses. The six verbs *describe*, *apply*, *explain*, *identify*, *understand*, and *evaluate* account for 50.2% of all verb uses. Verb frequency information is available in Table B-6.

articulate, assist, categorize, characterize, communicate, compute, conduct, decipher, detect, devise, diagram, document, draw, explore, handle, harden, illustrate, map, mitigate, monitor, organize, produce, protect, prototype, quantify, rate, recognize, resolve, review, select, set up, suggest, test, utilize

Table 2: verbs used only a single time

5. ANALYSIS AND DISCUSSION

The main benefit of this analysis is that the range

of academic burden across the 73 KUs becomes evident when viewed through the lens of curricular load scores. This begins to make clear why it might be worthwhile considering an alternative to 1 KU ≡ 1 KU.

The small graph in Figure 3 provides a sense of how the UCLS differs across all KUs, from the most lightweight KU, Systems Certification and Accreditation (SCA), with the fewest learning outcomes and topics and a UCLS of 7, to Hardware/Firmware Security (HFS), the KU with the most learning outcomes and topics and a UCLS of 46. A larger version of this graph is provided in Figure B-1.

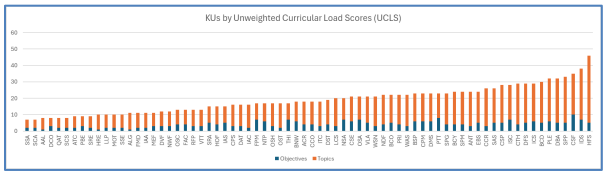


Figure 3: KUs by UCLS

Further comparisons of the KUs using WCLS, as in Figure 4, suggest that the academic burden difference among KUs is likely even greater. The weighting of learning outcomes reveals subtle differences among the KUs and shifts the ordering. While SCA remains the least complex KU with a WCLS of 8, Intrusion Detection/Prevention Systems (IDS) emerges as the most complex with a WCLS of 55. A larger version of this graph is provided in Figure B-2.

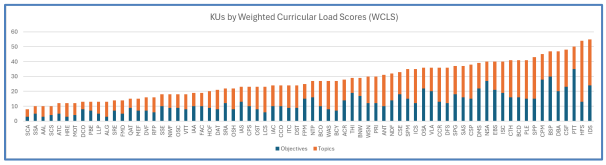


Figure 4: KUs by WCLS

Since topics are treated the same for UCLS and WCLS, the analysis can focus solely on the learning outcomes to gauge how scores change when Bloom weighting is included. Figure 5 shows the change from UCLS to WCLS calculations for each KU once weights are applied. The KU SCA shows the smallest variation, with an increase of just 1, while Penetration Testing (PTT) exhibits the largest change, jumping by 27 and shifting in order from the 20th most burdensome KU using UCLS to the 3rd biggest lift when considering WCLS. A larger version of this graph is provided in Figure B-3.

Limitations

While the results of this analysis appear promising, there are some shortcomings. First, if there is a weakness in the administrative guidance on viewing 1 KU ≡ 1 KU, the same weakness now exists when discussing learning outcomes (LO) and topics (T), albeit perhaps to a lesser degree. For both suggested techniques, the simplification shifts to 1 LO ≡ 1 LO or 1 LO at Bloom Level X ≡ 1 LO at Bloom Level X, and 1 T ≡ 1 T. The problem with the unweighted 1 LO ≡ 1 LO is readily apparent when comparing the KU Systems Certification and Accreditation (SCA) LO #2, "Define certification and accreditation" (Becker, et al, 2024, p. 108), with the KU Embedded Systems (EBS) LO #5, "Design, develop and prototype embedded system solutions that address specific real-world problems, integrating hardware and software components effectively" (p. 63). This problem is partly mitigated by weighting learning outcomes by Bloom level, but it remains a problem nonetheless.

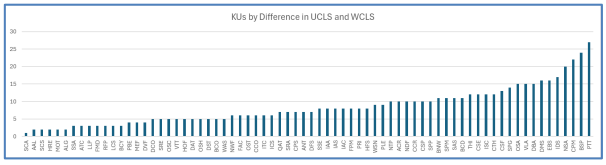


Figure 5: WCLS KUs Objective Difference from UCLS

An insidious limitation of WCLS is that LO weighting by Bloom level is ordinal, not interval. This means that it is inaccurate to consider an LO mapped to Bloom level 2 to be twice as difficult or burdensome as an LO mapped to Bloom level 1; and, by extension, we do not suggest that *creating* (Bloom level 6) is 6x more difficult than *remembering* (Bloom level 1). This can pose challenges when deriving insights from the rankings. It is crucial to remember that while the WCLS can be used to rank KUs, arithmetic operations should not be performed with it. Unfortunately, while both SCA (WCLS=8) and Supply Chain Security (SCS) (WCLS=10) are each less burdensome than Virtualization Technologies (VTT) (WCLS=18), this does not mean that SCA + SCS ≡ VTT.

When it comes to weighting, the key lies in effectively mapping verbs to Bloom's levels. That is why it is crucial for the chosen verbs to accurately represent those levels. This not only enhances clarity but also ensures that the assessments are meaningful and aligned with learning objectives.

Implications and Recommendations

This investigation suggests that the academic

burden of KUs, as indicated by unweighted and weighted curricular load scores, differs sufficiently that assuming 1 KU ≡ 1 KU is a bit tenuous. From this premise, a few suggestions are recommended:

1-that the NCAE-C program office consider forming a small task force to consider the feasibility and potential value of calculating the curricular load for KUs.

2-that the NCAE-C program office provide a Revised Bloom's Taxonomy chart of non-duplicated verbs as an appendix to the KU document for any verbs used to create KU learning outcomes – perhaps with the next document iteration.

3-a reduction in the number of verbs used across all KUs with a focus on picking verbs that have wide agreement for mapping to a particular Bloom level. In the absence of a universal, authoritative list of non-repeating verbs aligned to the revised Bloom's Taxonomy levels, it seems a good idea for significant collaborative efforts like the NCAE-C to limit the use of verbs to those that have high agreement for Bloom's level mapping.

4-that no verb be used for a single KU learning outcome. Any verb used in the KU document should be used widely.

5-that some verbs be avoided entirely to provide greater clarity of learning outcomes; e.g., leverage, "provide a summary" [summarize], contrast [see definition of compare].

6-that no learning outcome contains more than one action verb. The presence of multiple verbs, especially verbs that differ widely in Bloom category, created a problem for the WCLS method and likely causes confusion more generally.

6. CONCLUSIONS & FUTURE WORK

This paper suggests that using Knowledge Units (KUs) as an element in estimating curricular load equivalence may mask differences in the curricular burden across KUs. It is discussed that a calculation based on the underlying KU components (learning outcomes and topics) may provide greater insight and prove more useful. Two methods were described and discussed for quantifying KU curricular load: unweighted curricular load scores (UCLS) and weighted curricular load scores (WCLS). By calculating UCLS and WCLS and by documenting a transparent coding methodology, a practical tool is introduced. Though specifically used to analyze KUs under the NCAE-C program, this tool can be used more generally for curriculum mapping, course sequencing, and equitable distribution of academic content.

These measures can be adapted by any standards-aligned curriculum with defined outcomes and topics, and assist the academic units with program design and review.

Future Work

While the current research explores a measure of curricular load, future work should extend this concept to examine its pedagogical consequences. For example, higher UCLS or WCLS scores may necessitate longer instructional coverage or more complex assignments (e.g., labs versus quizzes), which directly affect course sequencing, credit hour allocation, and student workload. Investigating these connections could lead to a more equitable distribution of content across programs, improving both instructional planning and the student learning experience.

Future research should also explore empirical relationships between curricular load scores and student-centered outcomes. High-load KUs may correlate with performance gaps if faculty do not provide appropriate scaffolding or support. Building on computing education research showing that cognitive complexity strongly shapes student achievement and persistence, studies could examine how UCLS and WCLS align with grades, retention, and standardized assessment results. By connecting curricular load to instructional practices and performance data, this framework could evolve into a practical tool not only for accreditation and program design but also for advancing equity and student success in cybersecurity education.

7. REFERENCES

Application Process and Adjudication Rubric Cyber Defense Working Group. (2024, July). National Centers of Academic Excellence in Cybersecurity NCAE-C 2024 Designation Requirements and Application Process. 20240716_CAE2024_ CAE-CD_Designation_ Requirements_Ver1.19. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_designation_requirements.pdf

Bamkole, A., Geissler, M., Koumadi, K., Servin, C., Tang, C., & Tucker, C. S. (2023). Bloom's for Computing: Enhancing Bloom's Revised Taxonomy with Verbs for Computing

Disciplines. Association for Computing Machinery, New York, NY. https://ccecc.acm.org/files/publications/Blooms-for-Computing-20240814.pdf

Becker, A., Blum, Z., Burgin, K. Carlin, A., Chu, B., Cranford-Wesley, D., Frank, S., Ghosh, T., Hamman, S., Joyce, R., Keller S., Kohnke, A., Levy, Y., Liu, X., Manikas, T., McBride, S., Mierzwa, S., Miller, S., Magaishi, M., … Zanella, G. (2024, December 9). National Centers of Academic Excellence in Cybersecurity (NCAE-C) – Cyber Defense (CAE-CD) Knowledge Units (KUs). https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf

Bloom, B.S. (Ed.), Engelhart, M.D., Furst, E.J., Hill,W.H., & Krathwohl, D.R. (1956). Taxonomy of educational objectives: The classification of educational goals. Handbook 1: Cognitive domain. New York: David McKay.

Clark, U., Stoker, G., Vetter, R., (2020). Looking Ahead to CAE-CD Program Changes. Information Systems Education Journal18(1) pp 29-39. https://isedj.org/2020-18/n1/ISEDJv18n1p29.pdf

Das, S., Das Mandal, S. K., & Basu, A. (2022). Classification of action verbs of Bloom's taxonomy cognitive domain: An empirical study. Journal of Education, 202(4), 554-566. https://doi.org/10.1177/00220574211002199

ElJishi, Z., Abdel-Hameed, F. S., Khuddro, A., & Zayed, S. Y. (2024). Translating bloom's taxonomy action verb list into Arabic for teacher preparation programs: Challenges/Problems and solutions. International Journal of Education and Literacy Studies, 12(1), 295-303. https://journals.aiac.org.au/index.php/IJELS/article/viewFile/8032/5254

Krathwohl, D. R. (2002). A Revision of Bloom's Taxonomy: An Overview. Theory Into Practice, 41(4), 212–218. https://doi.org/10.1207/s15430421tip4104_2

Newton, P. M., Da Silva, A., & Peters, L. G. (2020, July). A pragmatic master list of action verbs for bloom's taxonomy. In Frontiers in Education (Vol. 5, p. 107). Frontiers Media SA. https://doi.org/10.3389/feduc.2020.00107

Stanny, C. J. (2016). Reevaluating Bloom's Taxonomy: What measurable verbs can and cannot say about student learning. Education Sciences, 6(4), 37. https://doi.org/10.3390/educsci6040037

Zhou, M., & Brown, D. (2015). Educational learning theories (2nd ed.). Education Open Textbooks. https://oer.galileo.usg.edu/education-textbooks/1

Appendix A

Knowledge	*f*	Understand	*f*	Apply	*f*	Analyze	*f*	Evaluate	*f*	Create	*f*
cite	17	classify	18	act	19	analyze	24	appraise	22	arrange	22
define	21	compare	11	apply	22	appraise	11	argue	12	assemble	14
describe	14	convert	13	calculate	10	categorize	19	assess	17	combine	14
identify	20	defend	12	choose	11	classify	10	choose	10	compose	19
label	21	describe	22	compute	10	compare	24	compare	18	construct	29
list	27	discuss	21	construct	13	contrast	19	conclude	13	create	19
locate	10	distinguish	12	demonstrate	20	criticize	11	criticize	11	design	24
match	14	estimate	11	dramatize	16	diagram	12	critique	14	develop	18
memorize	10	explain	28	employ	16	differentiate	20	defend	15	devise	13
name	22	express	17	illustrate	18	discriminate	11	estimate	15	formulate	18
outline	11	extend	11	interpret	15	distinguish	21	evaluate	16	generate	11
recall	24	generalize	11	manipulate	10	divide	12	judge	25	invent	10
recite	12	identify	14	modify	12	examine	18	manage	15	modify	10
recognize	14	infer	15	operate	17	infer	14	prepare	12	organize	21
record	13	interpret	17	practice	15	outline	10	rearrange	19	plan	21
relate	11	locate	10	prepare	11	point out	12	reconcile	12	prepare	12
repeat	20	paraphrase	22	produce	13	question	12	set up	15	produce	13
reproduce	11	predict	12	relate	12	relate	17	synthesize	16	rate	21
select	16	recognize	11	schedule	11	select	12			revise	12
state	23	report	10	show	13	separate	10			write	17
		restate	15	sketch	17	subdivide	10				
		review	15	solve	19	test	14				
		rewrite	12	use	25						
		summarize	20								
		translate	21								

Figure A-1: Stanny's Table 2 of 128 verbs; 104 unique, 18 duplicates (e.g., describe under Knowledge & Understand), 3 triplicates (e.g., relate under Knowledge, Apply, & Analyze). The f score indicates the number of lists out of 30 (2016, p. 7).

Evaluation	Rate, evaluate, assess, judge, justify
Synthesis	Create, compose, argue, design, plan, support, revise, formulate
Analysis	Analyze, question, differentiate, experiment, examine, test, categorize, distinguish, calculate, contrast, outline, infer, discriminate, compare
Application	Operate, apply, use, demonstrate, solve, produce, prepare, choose
Comprehension	Translate, paraphrase, discuss, report, locate, generalize, explain, classify, summarize
Knowledge	List, define, recall, state, label, repeat, name
Avoid	*appreciate, know, familiar, aware, understand, select, explain, relate, arrange, choose*

Figure A-2: Newton et al.'s Table 1 of 51 unique verbs compiled from 47 lists. Verbs appeared in more than half of the 47 lists and were in the same Bloom level for more than half of the lists in which they were included (2020, p. 4).

Knowledge	f	Comprehension	f	Application	f	Analysis	f	Evaluation	f	Create	f
Cite	17	convert	13	act	19	Analyze	24	argue	12	Arrange	22
Define	21	discuss	21	apply	22	categorize	19	assess	17	assemble	14
Label	21	explain	28	calculate	10	Contrast	19	conclude	13	combine	14
List	27	express	17	compute	10	Diagram	12	critique	14	compose	19
Match	14	extend	17	demonstrate	20	differentiate	20	evaluate	16	create	19
memorize	10	generalize	11	dramatize	16	discriminate	11	judge	25	design	24
Name	22	paraphrase	22	employ	16	Divide	12	manage	15	develop	18
Recall	24	predict	12	illustrate	18	Examine	18	rearrange	19	devise	13
Recite	12	report	10	manipulate	10	point out	12	reconcile	12	formulate	18
Record	13	restate	15	operate	17	Question	12	set up	15	generate	11
Repeat	20	review	15	practice	15	Separate	10	synthesize	16	invent	10
reproduce	11	rewrite	12	schedule	11	subdivide	10			organize	21
State	23	summarize	20	show	13	Test	14			plan	21
		translate	21	sketch	17					rate	21
				solve	19					revise	12
				use	25					write	17

Figure A-3: Das et al.'s Table 5 of 84 unique verbs derived from Stanny's Table 2 with repeated verbs removed (2022, p. 561).

Remembering	Understanding	Applying		Analyzing	Evaluating	Creating
Define	**Annotate**	Apply	Investigate	Analyze	**Adapt**	Assemble
Duplicate	Classify	**Backup**	**Iterate**	**Articulate**	**Administer**	**Collaborate**
Enumerate	**Comment**	**Build**	Manipulate	Attribute	Appraise	**Compose**
Find	Convert	Calculate	**Map**	**Automate**	Argue	Construct
Identify	Demonstrate	Carry out	Measure	Categorize	Assess	Create
Label	Describe	**Code**	Modify	Compare	Choose	Design
List	Differentiate	**Compile**	Operate	**Contextualize**	Critique	Develop
Locate	Discuss	**Compute**	Perform	Contrast	Debate	Devise
Memorize	Exemplify	**Configure**	Produce	**Correlate**	**Debug**	Formulate
Name	Explain	**Connect**	Provision	Decompose	**Decide**	**Generate**
Recall	Infer	**Decrypt**	Randomize	Deconstruct	Defend	Hypothesize
Recognize	Interpret	**Deploy**	Recover	Deduce	Estimate	Invent
Reference	Paraphrase	Diagram	Restore	**Detect**	Evaluate	Make
Retrieve	Report	**Document**	Schedule	Discriminate	Judge	Plan
Select	Summarize	Edit	Solve	Distinguish	Justify	**Program**
State	Translate	**Encrypt**	Store	Examine	**Optimize**	**Script**
		Execute	Train	**Generalize**	**Prioritize**	**Secure**
		Graph	Use	Integrate	**Prove**	**Visualize**
		Illustrate	Virtualize	**Model**	Support	
		Implement	Write	**Monitor**	Test	
		Install		Organize	**Validate**	
				Outline	Value	
				Predict	Verify	
				Simulate		
				Structure		
				Trace		
				Translate		
				Update		

Figure A-4: Bamkole et al.'s Bloom's for Computing list of 142 unique verbs, 56 of which are the new compute-related verbs (2023, p. 28).

	Action verbs
Remember تذكر	Find, cite, locate, recall, highlight, retrieve, search, define, describe, label, list, match, name, reproduce, state
Understand افهم	Annotate, outline, compare, discuss, convert, explain, extend, generalize, exemplify (give an example), paraphrase, predict, summarize, translate, research, review, restate
Apply طبّق	Apply, articulate, calculate, choose, complete, execute, dramatize, practice, share, change, illustrate, operate, teach, examine, classify, compute, demonstrate, discover, manipulate, prepare, produce, relate, show, solve, use
Analyze حلّل	Analyze, categorize, deduce, edit, investigate, reverse, select, separate, engineer, examine, establish, break down, conclude, diagram, deconstruct, differentiate, discriminate, distinguish, correlate, contrast
Evaluate قيّم	Argue, assess, collaborate, critique, debate, evaluate, hypothesize, judge, moderate, recommend, reflect, test, verify, prioritize, rate, inspect, decide, measure. appraise, conclude, criticize, defend, discriminates, justify, support
Create أبدع	Integrate, intervene, model, negotiate, plan, progress, rearrange, formulate, construct, reinforce, revise, structure, substitute, validate, assemble, develop, draft, invent, produce, propose, publish, repurpose, upload, write, synthesize, categorize, combine, compile, compose, create, devise, design, generate, organize, reconstruct, reorganize, rewrite, tell, identify

Figure A-5: ElJishi et al.'s Table 1 140-verb list with four duplicates across levels – categorize, conclude, examine, and produce (2024, p. 298).

Appendix B

List of Unique KU Verbs as Placed in Revised Bloom's Taxonomy Levels					
	ElJishi (2024)	**ACM (2023)**	**Das (2022)**	**Newton (2020)**	**Authors**
Remember					
define	x	x	x	x	
identify		x			
list	x	x	x	x	
recall	x	x	x	x	
recognize		x			
select		x			
Understand					
annotate	x	x			
communicate					x
describe					x
discuss	x	x	x	x	
explain	x	x	x	x	
explore					x
review	x		x		
understand					x
Apply					
apply	x	x	x	x	
assist					x
compute	x	x	x		
conduct					x
configure		x			
demonstrate	x		x	x	
deploy		x			
document		x			
draw					x
execute	x	x			
handle					x
harden					x
illustrate	x	x	x		
implement		x			
install		x			
leverage					x
map		x			
mitigate					x
perform		x			
produce		x		x	

protect					x
provide					x
quantify					x
use	x	x	x	x	
utilize					x
	ElJishi (2024)	**ACM (2023)**	**Das (2022)**	**Newton (2020)**	**Authors**
Analyze					
analyze	x	x	x	x	
articulate		x			
categorize		x	x	x	
characterize					x
compare		x		x	
contrast	x	x	x	x	
decipher					x
detect		x			
diagram	x		x		
differentiate	x		x	x	
examine		x	x	x	
monitor		x			
outline		x		x	
resolve					x
Evaluate					
assess	x	x	x	x	
determine					x
evaluate	x	x	x	x	
rate	x			x	
recommend	x				
set up			x		
suggest					x
test	x	x			
Create					
create	x	x	x	x	
design	x	x	x	x	
develop	x	x	x		
devise	x	x	x		
organize	x		x		
plan	x	x	x	x	
propose	x				
prototype					x
write	x		x		

Table B-1: reference for why verbs were placed in Bloom category

List of KUs Ordered by Unweighted Curricular Load Score (UCLS) UCLS = # of Learning Outcomes (LO) + # of Topics (T)							
KU	**LO**	**T**	**UCLS**	**KU**	**LO**	**T**	**UCLS**
Hardware/Firmware Security (HFS)	5	41	46	Introduction to Theory of Computation (ITC)	3	15	18
Intrusion Detection/Prevention Systems (IDS)	7	31	38	Fraud Prevention & Management (FPM)	7	10	17
Cybersecurity Fundamentals (CSF)	10	25	35	Threat Intelligence (THI)	7	10	17
Secure Programming Practices (SPP)	5	28	33	Network Technology & Protocols (NTP)	6	11	17
Policy, Legal, Ethics, and Compliance (PLE)	6	26	32	Operating Systems Hardening (OSH)	3	14	17
Data Administration (DBA)	5	27	32	Operating Systems Theory (OST)	2	15	17
Business Continuity and Disaster Recovery (BCD)	5	25	30	Cyber-Physical Systems (CPS)	3	13	16
Industrial Control Systems (ICS)	6	23	29	Databases (DAT)	3	13	16
Digital Forensics (DFS)	5	24	29	IA Compliance (IAC)	2	14	16
Cyber Threats (CTH)	4	25	29	Security Risk Analysis (SRA)	5	10	15
IT Systems Components (ISC)	7	21	28	IA Standards (IAS)	5	10	15
Cybersecurity Principles (CSP)	5	23	28	Host Forensics (HOF)	4	11	15
Software Assurance (SAS)	5	21	26	Operating Systems Concepts (OSC)	4	9	13
Cyber Crime (CCR)	3	23	26	Forensic Accounting (FAC)	4	9	13
Embedded Systems (EBS)	5	19	24	Radio Frequency Principles (RFP)	3	10	13
Basic Cryptography (BCY)	4	20	24	Virtualization Technologies (VTT)	3	10	13
Security Program Management (SPM)	4	20	24	Device Forensics (DVF)	3	9	12
Advanced Network Technology & Protocols (ANT)	3	21	24	Network Forensics (NWF)	3	9	12
Penetration Testing (PTT)	8	15	23	Media Forensics (MEF)	3	8	11
Basic Scripting and Programming (BSP)	6	17	23	Formal Methods (FMD)	2	9	11
Cybersecurity Planning and Management (CPM)	6	17	23	IA Architectures (IAA)	2	9	11
Database Management Systems (DMS)	6	17	23	Algorithms (ALG)	1	10	11
Systems Programming (SPG)	4	19	23	Low Level Programming (LLP)	2	8	10
Basic Cyber Operations (BCO)	5	17	22	Mobile Technologies (MOT)	2	8	10
Network Defense (NDF)	4	18	22	Systems Security Engineering (SSE)	2	8	10
Privacy (PRI)	4	18	22	Hardware Reverse Engineering (HRE)	1	9	10
Web Application Security (WAS)	3	19	22	Pre-OS Boot Environment (PBE)	3	6	9
Operating Systems Administration (OSA)	7	14	21	Analog Telecommunications (ATC)	2	7	9
Cybersecurity Ethics (CSE)	6	15	21	Software Reverse Engineering (SRE)	2	7	9
Vulnerability Analysis (VLA)	5	16	21	Digital Communications (DCO)	3	5	8
Wireless Sensor Networks (WSN)	3	18	21	QA/Functional Testing (QAT)	2	6	8
Network Security Administration (NSA)	7	13	20	Supply Chain Security (SCS)	2	6	8
Life-Cycle Security (LCS)	3	17	20	Advanced Algorithms (AAL)	1	7	8
Data Structures (DST)	4	15	19	Software Security Analysis (SSA)	2	5	7
Basic Networking (BNW)	6	12	18	Systems Certification & Accreditation (SCA)	2	5	7
Advanced Cryptography (ACR)	4	14	18	Independent/Directed Study/Research (IDR)			N/A
Cloud Computing (CCO)	4	14	18				

Table B-2: List of all 73 KUs ordered by UCLS

List of KUs Ordered by Weighted Curricular Load Score (WCLS)							
KU	**LO**	**T**	**WCLS**	**KU**	**LO**	**T**	**WCLS**
Intrusion Detection/Prevention Systems (IDS)	7	31	55	Cloud Computing (CCO)	4	14	24
Hardware/Firmware Security (HFS)	5	41	54	IA Compliance (IAC)	2	14	24
Penetration Testing (PTT)	8	15	50	Data Structures (DST)	4	15	24
Cybersecurity Fundamentals (CSF)	10	25	48	Introduction to Theory of Computation (ITC)	3	15	24
Basic Scripting and Programming (BSP)	6	17	47	IA Standards (IAS)	5	10	23
Data Administration (DBA)	5	27	47	Cyber-Physical Systems (CPS)	3	13	23
Cybersecurity Planning and Management (CPM)	6	17	45	Operating Systems Theory (OST)	2	15	23
Secure Programming Practices (SPP)	5	28	43	Life-Cycle Security (LCS)	3	17	23
Business Continuity and Disaster Recovery (BCD)	5	25	41	Security Risk Analysis (SRA)	5	10	22
Cyber Threats (CTH)	4	25	41	Operating Systems Hardening (OSH)	3	14	22
Policy, Legal, Ethics, and Compliance (PLE)	6	26	41	Databases (DAT)	3	13	21
Network Security Administration (NSA)	7	13	40	Host Forensics (HOF)	4	11	20
Embedded Systems (EBS)	5	19	40	Forensic Accounting (FAC)	4	9	19
IT Systems Components (ISC)	7	21	40	IA Architectures (IAA)	2	9	19
Database Management Systems (DMS)	6	17	39	Systems Security Engineering (SSE)	2	8	18
Cybersecurity Principles (CSP)	5	23	38	Operating Systems Concepts (OSC)	4	9	18
Systems Programming (SPG)	4	19	37	Network Forensics (NWF)	3	9	18
Software Assurance (SAS)	5	21	37	Virtualization Technologies (VTT)	3	10	18
Operating Systems Administration (OSA)	7	14	36	Device Forensics (DVF)	3	9	16
Vulnerability Analysis (VLA)	5	16	36	Radio Frequency Principles (RFP)	3	10	16
Cyber Crime (CCR)	3	23	36	QA/Functional Testing (QAT)	2	6	15
Digital Forensics (DFS)	5	24	36	Media Forensics (MEF)	3	8	15
Security Program Management (SPM)	4	20	35	Software Reverse Engineering (SRE)	2	7	14
Industrial Control Systems (ICS)	6	23	35	Formal Methods (FMD)	2	9	14
Cybersecurity Ethics (CSE)	6	15	33	Digital Communications (DCO)	3	5	13
Network Defense (NDF)	4	18	32	Pre-OS Boot Environment (PBE)	3	6	13
Advanced Network Technology & Protocols (ANT)	3	21	31	Low Level Programming (LLP)	2	8	13
Privacy (PRI)	4	18	30	Algorithms (ALG)	1	10	13
Wireless Sensor Networks (WSN)	3	18	30	Analog Telecommunications (ATC)	2	7	12
Threat Intelligence (THI)	7	10	29	Mobile Technologies (MOT)	2	8	12
Basic Networking (BNW)	6	12	29	Hardware Reverse Engineering (HRE)	1	9	12
Advanced Cryptography (ACR)	4	14	28	Software Security Analysis (SSA)	2	5	10
Network Technology & Protocols (NTP)	6	11	27	Supply Chain Security (SCS)	2	6	10
Basic Cyber Operations (BCO)	5	17	27	Advanced Algorithms (AAL)	1	7	10
Web Application Security (WAS)	3	19	27	Systems Certification & Accreditation (SCA)	2	5	8
Basic Cryptography (BCY)	4	20	27	Independent/Directed Study/Research (IDR)			N/A
Fraud Prevention & Management (FPM)	7	10	25				

Table B-3: List of all 73 KUs ordered by WCLS

List of KUs and Learning Objective Verbs Used for Weighting Ordered by Verb Weight			
KU	**LO**	**Verb weight**	**LO Verbs Used for Weighting**
Penetration Testing (PTT)	8	35	plan, analyze, discuss, describe, create, devise, assess, compare
Basic Scripting and Programming (BSP)	6	30	write, write, write, write, implement, demonstrate
Cybersecurity Planning and Management (CPM)	6	28	examine, develop, develop, outline, discuss, develop
Network Security Administration (NSA)	7	27	recommend, recommend, protect, monitor, assist, evaluate, discuss
Intrusion Detection/Prevention Systems (IDS)	7	24	detect, apply, apply, leverage, apply, test, apply
Cybersecurity Fundamentals (CSF)	10	23	define, describe, describe, describe, evaluate, describe, describe, apply, describe, discuss
Database Management Systems (DMS)	6	22	compare, describe, apply, apply, outline, design
Operating Systems Administration (OSA)	7	22	set up, configure, configure, perform, install, review, configure
Embedded Systems (EBS)	5	21	describe, explain, develop, evaluate, design
Data Administration (DBA)	5	20	draw, evaluate, examine, compare, outline
Vulnerability Analysis (VLA)	5	20	apply, create, apply, propose, explain
IT Systems Components (ISC)	7	19	differentiate, characterize, describe, understand, understand, describe, apply
Threat Intelligence (THI)	7	19	identify, perform, apply, demonstrate, demonstrate, apply, apply
Systems Programming (SPG)	4	18	develop, apply, implement, develop
Cybersecurity Ethics (CSE)	6	18	explain, examine, describe, identify, examine, assess
Basic Networking (BNW)	6	17	describe, apply, apply, apply, examine, describe
Cyber Threats (CTH)	4	16	compare, rate, evaluate, explain
Business Continuity and Disaster Recovery (BCD)	5	16	identify, explain, implement, suggest, evaluate
Software Assurance (SAS)	5	16	apply, describe, create, apply, explain
Network Technology & Protocols (NTP)	6	16	demonstrate, demonstrate, describe, mitigate, demonstrate, explain
Security Program Management (SPM)	4	15	apply, apply, assess, articulate
Cybersecurity Principles (CSP)	5	15	differentiate, describe, analyze, apply, understand
Secure Programming Practices (SPP)	5	15	produce, describe, understand, differentiate, examine
Policy, Legal, Ethics, and Compliance (PLE)	6	15	describe, describe, differentiate, explain, explain, apply
Fraud Prevention & Management (FPM)	7	15	describe, describe, analyze, describe, describe, describe, recognize
Network Defense (NDF)	4	14	describe, explain, evaluate, evaluate
Advanced Cryptography (ACR)	4	14	explain, evaluate, explain, evaluate
Cyber Crime (CCR)	3	13	examine, evaluate, examine
Hardware/Firmware Security (HFS)	5	13	outline, use, describe, describe, discuss
IA Standards (IAS)	5	13	compare, map, describe, describe, describe
Wireless Sensor Networks (WSN)	3	12	diagram, describe, propose
Privacy (PRI)	4	12	examine, explore, describe, compare
Security Risk Analysis (SRA)	5	12	describe, describe, evaluate, identify, annotate
Digital Forensics (DFS)	5	12	discuss, describe, describe, use, perform
Industrial Control Systems (ICS)	6	12	identify, describe, describe, apply, explain, explain
IA Architectures (IAA)	2	10	examine, design
IA Compliance (IAC)	2	10	compare, plan

Systems Security Engineering (SSE)	2	10	determine, determine
Advanced Network Technology & Protocols (ANT)	3	10	describe, describe, develop
Cyber-Physical Systems (CPS)	3	10	describe, implement, evaluate
Cloud Computing (CCO)	4	10	compare, list, explain, apply
Forensic Accounting (FAC)	4	10	describe, implement, describe, compute
Basic Cyber Operations (BCO)	5	10	describe, describe, identify, describe, use
QA/Functional Testing (QAT)	2	9	develop, perform
Introduction to Theory of Computation (ITC)	3	9	describe, differentiate, quantify
Network Forensics (NWF)	3	9	describe, analyze, use
Operating Systems Concepts (OSC)	4	9	describe, describe, describe, install
Data Structures (DST)	4	9	list, discuss, utilize, implement
Host Forensics (HOF)	4	9	discuss, describe, describe, perform
Operating Systems Theory (OST)	2	8	understand, design
Databases (DAT)	3	8	describe, outline, describe
Digital Communications (DCO)	3	8	describe, describe, compare
Operating Systems Hardening (OSH)	3	8	describe, install, leverage
Virtualization Technologies (VTT)	3	8	describe, compare, discuss
Web Application Security (WAS)	3	8	examine, describe, explain
Software Reverse Engineering (SRE)	2	7	apply, analyze
Device Forensics (DVF)	3	7	describe, perform, explain
Media Forensics (MEF)	3	7	describe, apply, explain
Pre-OS Boot Environment (PBE)	3	7	describe, describe, demonstrate
Basic Cryptography (BCY)	4	7	identify, describe, describe, describe
Life-Cycle Security (LCS)	3	6	describe, describe, describe
Radio Frequency Principles (RFP)	3	6	understand, understand, discuss
Analog Telecommunications (ATC)	2	5	illustrate, understand
Formal Methods (FMD)	2	5	apply, describe
Low Level Programming (LLP)	2	5	apply, explain
Software Security Analysis (SSA)	2	5	describe, apply
Mobile Technologies (MOT)	2	4	understand, describe
Supply Chain Security (SCS)	2	4	describe, describe
Advanced Algorithms (AAL)	1	3	implement
Algorithms (ALG)	1	3	implement
Hardware Reverse Engineering (HRE)	1	3	perform
Systems Certification & Accreditation (SCA)	2	3	describe, define
Independent/Directed Study/Research (IDR)		N/A	

Table B-4: verbs and verb weighting used for each KU for the WCLS calculation; e.g., the KU

List of KU Learning Outcomes (LO) with Multiple Verbs; with Verbs Unused for Weighting Identified E.g., CSF LO #5 has verbs describe & evaluate; from Table B-1, describe is Bloom Level 2, evaluate is Bloom Level 5, so evaluate is used when calculating the WCLS			
KU	**LO#**	**All Verbs**	**Verbs Unused for Weighting**
Cybersecurity Fundamentals (CSF)	5	describe, evaluate	describe
Cybersecurity Principles (CSP)	1	differentiate, discuss	discuss
Cybersecurity Principles (CSP)	3	analyze, identify	identify
Cybersecurity Principles (CSP)	4	identify, apply	identify
IT Systems Components (ISC)	1	differentiate, diagram	differentiate
Basic Networking (BNW)	1	describe, explain	explain
Basic Networking (BNW)	3	apply, demonstrate	demonstrate
Basic Networking (BNW)	4	apply, demonstrate	demonstrate
Basic Networking (BNW)	5	perform, examine	perform
Basic Scripting and Programming (BSP)	1	write, execute	execute
Basic Scripting and Programming (BSP)	2	write, execute	execute
Basic Scripting and Programming (BSP)	3	write, execute	execute
Basic Scripting and Programming (BSP)	4	write, execute	execute
Network Defense (NDF)	1	describe, discuss	discuss
Network Defense (NDF)	2	explain, discuss	explain
Network Defense (NDF)	3	analyze, evaluate	analyze
Operating Systems Concepts (OSC)	1	describe, discuss	describe
Operating Systems Concepts (OSC)	2	describe, discuss	describe
Operating Systems Concepts (OSC)	3	identify, describe	identify
Operating Systems Concepts (OSC)	4	install, configure, harden	configure, harden
Cyber Threats (CTH)	1	identify, compare, contrast	identify, compare
Cyber Threats (CTH)	2	communicate, rate, describe	communicate, describe
Cyber Threats (CTH)	4	explain, discuss	explain
Cybersecurity Planning and Management (CPM)	1	examine, describe	describe
Cybersecurity Planning and Management (CPM)	4	outline, explain	explain
Policy, Legal, Ethics, and Compliance (PLE)	1	identify, recall, describe	identify, recall
Policy, Legal, Ethics, and Compliance (PLE)	3	describe, differentiate	describe
Security Risk Analysis (SRA)	1	describe, explain	describe
Security Risk Analysis (SRA)	3	evaluate, categorize, recommend	evaluate, categorize
Security Risk Analysis (SRA)	4	identify, select	select
Security Risk Analysis (SRA)	5	annotate, apply	annotate
Advanced Algorithms (AAL)	1	understand, implement	understand
Advanced Cryptography (ACR)	4	evaluate, explain	explain
Advanced Network Technology & Protocols (ANT)	1	identify, describe	identify
Advanced Network Technology & Protocols (ANT)	2	describe, discuss	discuss
Algorithms (ALG)	1	understand, implement	understand
Analog Telecommunications (ATC)	1	describe, illustrate	describe

Analog Telecommunications (ATC)	2	understand, describe	understand
Business Continuity and Disaster Recovery (BCD)	2	explain, describe	explain
Business Continuity and Disaster Recovery (BCD)	4	analyze, suggest	analyze
Business Continuity and Disaster Recovery (BCD)	5	evaluate, recommend	recommend
Basic Cyber Operations (BCO)	2	list, describe	list
Cloud Computing (CCO)	4	describe, apply	describe
Cyber-Physical Systems (CPS)	3	analyze, evaluate	analyze
Cybersecurity Ethics (CSE)	4	identify, recall	recall
Cybersecurity Ethics (CSE)	5	examine, differentiate	differentiate
Data Administration (DBA)	1	draw, describe	describe
Data Administration (DBA)	2	define, evaluate	define
Data Administration (DBA)	4	compare, contrast	contrast
Database Management Systems (DMS)	1	compare, contrast	contrast
Database Management Systems (DMS)	4	describe, apply	describe
Database Management Systems (DMS)	6	design, deploy	deploy
Databases (DAT)	3	identify, describe	identify
Device Forensics (DVF)	2	perform, handle, understand	handle, understand
Digital Communications (DCO)	3	compare, contrast, describe	contrast, describe
Digital Forensics (DFS)	2	identify, describe	identify
Embedded Systems (EBS)	1	identify, describe	identify
Embedded Systems (EBS)	3	develop, implement	implement
Embedded Systems (EBS)	5	design, develop, prototype	develop, prototype
Forensic Accounting (FAC)	2	describe, implement	implement
Hardware/Firmware Security (HFS)	2	explain, use	explain
Host Forensics (HOF)	4	perform, provide	provide
IA Architectures (IAA)	1	examine, identify	identify
IA Compliance (IAC)	1	compare, contrast	contrast
IA Compliance (IAC)	2	plan, conduct	conduct
IA Standards (IAS)	1	compare, contrast	contrast
IA Standards (IAS)	5	list, describe	list
Industrial Control Systems (ICS)	1	identify, recall	identify
Introduction to Theory of Computation (ITC)	3	describe, quantify	describe
Intrusion Detection/Prevention Systems (IDS)	1	detect, identify, resolve, document	identify, resolve, document
Intrusion Detection/Prevention Systems (IDS)	6	deploy, test	deploy
Life-Cycle Security (LCS)	2	list, describe, explain	list, describe
Life-Cycle Security (LCS)	3	list, describe	list
Mobile Technologies (MOT)	1	understand, explain	understand
Network Forensics (NWF)	2	analyze, decipher, identify, provide	decipher, identify, provide
Network Security Administration (NSA)	1	analyze, recommend	analyze
Network Security Administration (NSA)	6	evaluate, perform	perform

Network Technology & Protocols (NTP)	3	identify, describe	identify
Network Technology & Protocols (NTP)	4	identify, mitigate	identify
Operating Systems Theory (OST)	2	understand, design, implement	understand, implement
Penetration Testing (PTT)	1	plan, organize, perform	organize, perform
Penetration Testing (PTT)	7	assess, determine	determine
Penetration Testing (PTT)	8	compare, contrast	contrast
Privacy (PRI)	4	compare, contrast	contrast
Radio Frequency Principles (RFP)	1	understand, identify	identify
Radio Frequency Principles (RFP)	2	understand, identify	identify
Systems Programming (SPG)	2	outline, apply	apply
Systems Security Engineering (SSE)	1	analyze, determine	analyze
Systems Security Engineering (SSE)	2	analyze, determine	analyze
Virtualization Technologies (VTT)	2	compare, contrast	contrast
Vulnerability Analysis (VLA)	2	create, apply	apply
Vulnerability Analysis (VLA)	4	propose, analyze	analyze
Wireless Sensor Networks (WSN)	1	diagram, deploy	deploy
Wireless Sensor Networks (WSN)	3	analyze, propose	analyze

Table B-5: list of KU Learning Outcomes with multiple verbs identifying which verbs were not used for the weighting when calculating WCLS

List of 70 Unique Verbs Used Across the 73 KUs Ordered by Frequency of Use (402 total verb uses)						
Verb	**# Times Used**	**% Verb Uses**		**Verb**	**# Times Used**	**% Verb Uses**
describe	91	22.6%		recall	2	0.5%
apply	32	8.0%		articulate	1	0.2%
explain	26	6.5%		assist	1	0.2%
identify	24	6.0%		categorize	1	0.2%
understand	15	3.7%		characterize	1	0.2%
evaluate	14	3.5%		communicate	1	0.2%
analyze	13	3.2%		compute	1	0.2%
discuss	13	3.2%		conduct	1	0.2%
compare	11	2.7%		decipher	1	0.2%
examine	11	2.7%		detect	1	0.2%
implement	11	2.7%		devise	1	0.2%
perform	10	2.5%		diagram	1	0.2%
demonstrate	9	2.2%		document	1	0.2%
develop	9	2.2%		draw	1	0.2%
contrast	8	2.0%		explore	1	0.2%
differentiate	7	1.7%		handle	1	0.2%
list	6	1.5%		harden	1	0.2%
outline	5	1.2%		illustrate	1	0.2%
configure	4	1.0%		map	1	0.2%
design	4	1.0%		mitigate	1	0.2%
execute	4	1.0%		monitor	1	0.2%
use	4	1.0%		organize	1	0.2%
write	4	1.0%		produce	1	0.2%
assess	3	0.7%		protect	1	0.2%
create	3	0.7%		prototype	1	0.2%
define	3	0.7%		quantify	1	0.2%
deploy	3	0.7%		rate	1	0.2%
determine	3	0.7%		recognize	1	0.2%
install	3	0.7%		resolve	1	0.2%
recommend	3	0.7%		review	1	0.2%
annotate	2	0.5%		select	1	0.2%
leverage	2	0.5%		set up	1	0.2%
plan	2	0.5%		suggest	1	0.2%
propose	2	0.5%		test	1	0.2%
provide	2	0.5%		utilize	1	0.2%

Table B-6: frequency of use across 73 KUs for all 70 unique verbs

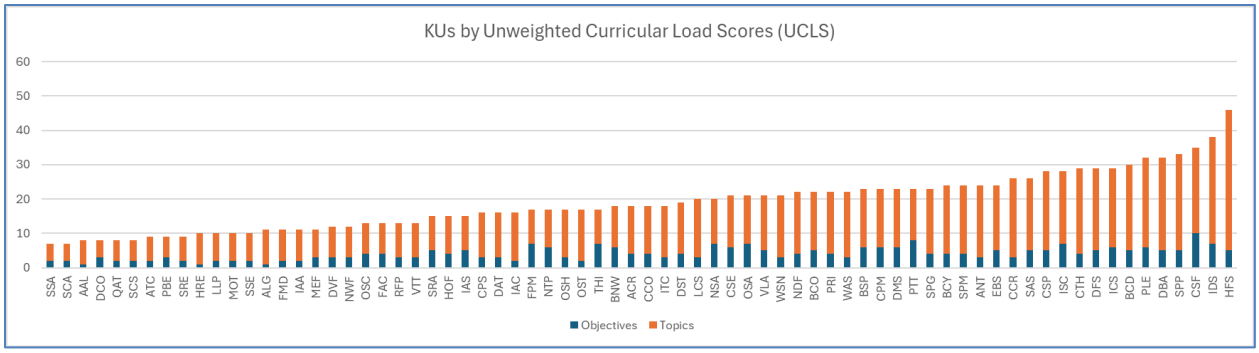


Figure B-1: KUs arranged from low to high UCLS

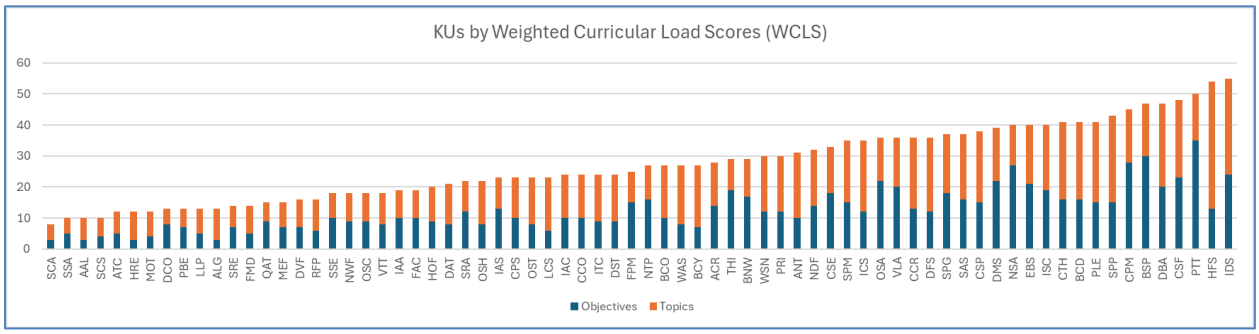


Figure B-2: KUs arranged from low to high WCLS

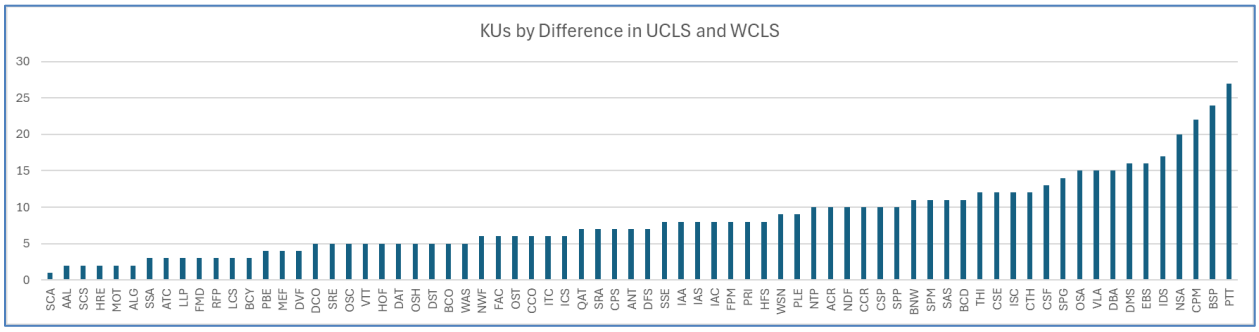


Figure B-3: KUs arranged from low to high by the change in UCLS to WCLS

Arizona's CyberSupply: Identifying Gateway-to-Cybersecurity and Cybersecurity Courses and Pathways in Secondary Education

Paul Wagner
paulewagner@arizona.edu

Robert Honomichl
rjhonomichl@arizona.edu

Crystal Beasley
crbeasley@arizona.edu

Thomas Reid
thomasreid1@arizona.edu

Logan Bradford
lbradford@arizona.edu

Alexandra Urbaszewski
aurbaszewski@azdohs.gov

College of Information Science
University of Arizona
Tucson, Arizona 85747, USA

Abstract

As cybersecurity threats continue to increase in sophistication, frequency, and scale, the demand for a skilled cybersecurity workforce expands. While post-secondary institutions have increased the number of cybersecurity programs, similar growth within high schools has not kept up. High school cybersecurity and computing courses are necessary to develop skills, raise awareness and digital responsibility, introduce career opportunities, and foster critical thinking and problem-solving skills. The CyberSupply data collection was part of the 2020 National Centers for Academic Excellence in Cybersecurity High School Designation Feasibility Study, initially focusing on availability and access to high school cybersecurity courses across 12 states. In 2023, the CyberSupply data collection was expanded to include Arizona. This paper provides an overview of the CyberSupply data collection project and details the Arizona CyberSupply data collection project conducted in fall 2023. Arizona's data is analyzed to identify the profile of Arizona schools and students, key findings, and opportunities for changing access to cybersecurity education in Arizona. These insights can help cybersecurity educators identify availability and access to cybersecurity courses and pathways in their states, areas of opportunities to support K-12 educators, course and pathway development opportunities, and address the cybersecurity workforce needs of the nation.

Keywords: Cybersecurity, Cybersecurity Education, CyberSupply, K-12 Education, Skills Gap, Pathways

Recommended Citation: Wagner, P., Honomichl, R., Beasley, C., Reid, T., Bradford, L., Urbaszewski, A., (2026). Arizona's CyberSupply: Identifying Gateway-to-Cybersecurity and Cybersecurity Courses and Pathways in Secondary Education. *Cybersecurity Pedagogy and Practice Journal;* v5(n1) pp 41-51. DOI# https://doi.org/10.62273/QPFS6373

Arizona's CyberSupply: Identifying Gateway-to-Cybersecurity and Cybersecurity Courses and Pathways in Secondary Education

Paul Wagner, Robert Honomichl, Crystal Beasley,
Thomas Reid, Logan Bradford and Alexandra Urbaszewski

1. INTRODUCTION

The cybersecurity skills and workforce gap continue to widen as the threat landscape continues to evolve at an alarming rate. The ability to overcome these issues requires a comprehensive cybersecurity education and training strategy. Collegiate cybersecurity programs continue to increase in availability and access due to increasing demand and support from federal agencies and funding. Despite this growth at post-secondary institutions, cybersecurity education within high schools is somewhat bare, with some pockets of growth (Dark et al., 2020). Only 16% of regular public high schools are estimated to have cybersecurity courses (Dark et al., 2020). The availability of cybersecurity courses is limited due to the availability of qualified teachers, availability of computer labs, crowded curriculum, and sequencing and scheduling. This limits access to cybersecurity courses to an estimated 3.7% of U.S. high school students (Dark et al., 2020). High school cybersecurity programs are important because they provide early skill development, help address the growing demand for cybersecurity professionals, raise awareness and promote responsible digital behavior, introduce diverse career opportunities, develop critical thinking and problem-solving skills, enhance national security, and bridge the digital divide. An added benefit is that these skills transcend the cybersecurity discipline. This paper provides an overview of the CyberSupply data collection project and details the Arizona CyberSupply data collection project conducted in fall 2023. Arizona's data is analyzed to identify the profile of Arizona schools and students and identify key findings and opportunities for changing access to cybersecurity education in Arizona. These insights can help cybersecurity educators identify the availability and access to cybersecurity courses and pathways in their states, identify areas of opportunities to support K-12 educators, course and pathway development, and address the cybersecurity workforce needs of the nation.

2. LITERATURE REVIEW

Cybersecurity Workforce Gap

The cybersecurity workforce shortage continues to be a concern, with over 450,000 unfilled positions within the United States (CyberSeek, 2025) and nearly four million globally (ISC2, 2023). Additionally, the cybersecurity threat continues to grow in sophistication, frequency, and scale, increasing stress on the cybersecurity workforce and leading to high employee turnover. White & Bunce (2023) estimates that nearly 51% of cybersecurity professionals will leave the field due to stressors like staffing and resource limitations, rising complexity of technology, remote work challenges, and compliance and regulatory pressures.

Compounding this problem is the increasing dissatisfaction of employers regarding the knowledge, skills, and abilities of cybersecurity graduates' capacity to fulfill the required tasks of the organization. Ross and Duke (2018) stated, "employers are expressing increasing concern about the relevance of certain cybersecurity-related education programs in meeting the real needs of their organization," in a report to the President of the United States. Additionally, an ISACA report (2023) identified that only 28% of employers surveyed believed that recent cybersecurity graduates were well prepared to meet the cybersecurity challenges of the organization, citing a lack of technical and soft skills. Addressing these concerns requires reviewing cybersecurity programs at the post-secondary level to ensure alignment with industry needs. Additionally, understanding the cybersecurity availability and access at the secondary education level can identify ways to develop competencies earlier in students' educational journey.

Collegiate Cybersecurity Programs

Hundreds of post-secondary institutions provide academic programs in cybersecurity to address the cybersecurity workforce gap and meet the knowledge, skills, and abilities required by employers. The National Security Agency's (NSA) National Cryptologic School partners with several federal partners on the National Centers of

Academic Excellence in Cybersecurity (NCAE-C) program. NCAE-C aims to create and manage a collaborative cybersecurity educational program with post-secondary institutions that:

- Establishes standards for cybersecurity curriculum and academic excellence;
- Includes competency development among students and faculty;
- Values community outreach and leadership in professional development;
- Integrates cybersecurity practice within the institution across disciplines; and
- Actively engages in solutions to challenges facing cybersecurity education (National Security Agency [NSA], 2025).

Currently, 467 institutions (National Centers of Academic Excellence in Cybersecurity [NCAE-C], 2025) maintain one or more of three designations: Cyber Defense, Cyber Operations, and/or Cyber Research. Institutions must complete a program of study validation that meets the desired characteristics required by the program office to produce the qualified workforce needed by the nation (NSA, 2025).

Alternatively, ABET is a nonprofit, non-governmental organization that accredits programs globally. They currently accredit 4,773 programs at 930 colleges and universities in 42 countries (ABET, 2025a). Similar to NCAE-C institutions, ABET-accredited programs ensure that graduates are prepared to enter the global workforce. ABET accredits programs in cybersecurity and similarly named computing programs and cybersecurity engineering and similarly named engineering programs. There are currently 54 institutions with one or both of these accreditations (ABET, 2025b).

It is important to note that additional schools not listed in these databases may also have cybersecurity programs. Additionally, colleges and universities may hold both ABET and NCAE-C designations.

High School Cybersecurity Programs

The availability and access of high school programs are difficult to identify. The National Center for Education Statistics (NCES) is the Department of Education's agency focused on collecting, compiling, analyzing, and reporting the condition of American education (National Center for Education Statistics [NCES], 2025). School statistical data provided by NCES includes directory information, school details, and enrollment characteristics; however, program information is not provided. Aggregate data for programs is typically collected by organizations and nonprofits at the local, state, or federal levels. Identifying program and course availability required the manual inspection of school websites. This is noteworthy as the process is time-intensive and can lead to errors.

Dark et al. (2020) conducted a study to identify (1) the availability of gateway-to-cybersecurity and cybersecurity courses and pathways and (2) the level of access to cybersecurity courses and pathways for 9-12 grade students in the U.S. This comprehensive study of 5,915 regular public high schools (42.5% of schools) and 192 Career and Technical Education (CTE) centers (15.8% of centers) located in Arkansas, Colorado, Florida, Georgia, Illinois, Maryland, Ohio, South Carolina, Texas, Utah, and Virginia provided a confidence level of >99.99% for public schools and 90% for CTE Centers (Dark et al., 2020).

CyberSupply's background and details on the methodology are outlined in the next section. Comprehensive study results can be found in the 2020 NCAE-C High School Designation Feasibility Study (Dark et al., 2020) with compiled results found at CyberSupply.org (Dark Enterprises, 2023). The CyberSupply study provided the template for Arizona's CyberSupply data collection project, which is the focus of this paper.

3. CYBERSUPPLY

Background

CyberSupply was part of the 2020 National Centers for Academic Excellence in Cybersecurity (NCAE-C) High School Designation Feasibility Study. The High School Feasibility study investigated the practicality of a high school cybersecurity recognition program by conducting a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis, identifying resources required to implement, and establishing a prospectus for success (Dark et al., 2020). The goals were to identify the availability, attendance, and access to gateway, non-gateway, and cybersecurity courses within public high schools and CTE centers within the U.S.

A gateway course is typically considered the first credit-bearing course in a program of study, which generally applies to the requirements of a degree program (Kwak, 2020). Alternatively, gateway courses can be considered courses that students take, such as English or biology. The CyberSupply study defined gateway courses as "introductory courses that teach necessary prerequisite knowledge that set students up for success during their academic career and their professional lives." (Dark et al., 2020, p.58) The

study further coded gateway courses as Computer Science (CS) gateway or Information Technology (IT) gateway. Table 1 outlines the courses used within the study.

CS Gateway	IT Gateway	Non-Gateway
CSP/AP CSP	IT Fundamentals	Computer Applications
CSP/AP CSA	Networking I	Computer Management and Support
CS Discoveries	Networking II	Database
CS Essentials	Networking III	Digital Media
Exploring CS		Game Design I
Intro to CS		Game Design II
Linux		Mobile Applications
Programming I		Robotics
Programming II		Web Design I
Programming III		Web Design II
		Capstone I
		Capstone

Table 1 – Course Coding (Dark et al., 2020)

Cyber.org's K-12 Cybersecurity Learning Standards (2021) center on three core themes: Computing Systems (CS), Digital Citizenship (DC), and Security (SEC). Within these themes are fundamentals in cybersecurity education focusing on communication and networking, hardware, software, online safety, ethics, policy and legal issues, information security, network security, and physical security (Cyber.org, Cyber Innovation Center, & Cybersecurity and Infrastructure Security Agency, 2021). Additionally, the High School Cybersecurity Curriculum Guidelines & Glossary (Teach Cyber, 2021) are based on four levels: big ideas, enduring understandings, learning objectives, and essential knowledge statements. The big ideas are broad areas of importance within cybersecurity, including ethics, establishing trust, ubiquitous connectivity, data security, system security, adversarial thinking, risk, and implications (Teach Cyber, 2021). In addition to these documents, concepts from the Cybersecurity Curricular Guidelines (ACM, 2017) and the Centers of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units (KUs) (Becker et al., 2024) were used to identify cybersecurity courses offered at schools within the study population. The following course titles were identified: Cybersecurity I, Cybersecurity II, Cybersecurity III, Principles of Cybersecurity, Network Security, Cyber Forensics, Cyber Ops, and Advanced Cyber Forensics (Dark et al., 2020).

Research questions were broken down into availability (the provision of courses in schools) and attendance and access (student access to courses in schools). Availability generally means that something can be used or obtained. For this study, availability of courses means that the course is listed within the school's academic catalog. Dark (2020) noted that merely listing a course in a school's catalog does not guarantee that the course has been or is being offered. Access generally refers to the ability to obtain or use a resource. Within this study, access is a function of the percentage of schools with gateway or cybersecurity courses, the number of students served in those schools per year, the number of courses available to those students, and the number of students that could be served with those courses (Dark et al., 2020). The following research questions guided the research study:

Availability

1) What percentage of schools and CTE centers have cybersecurity courses and computing courses that would be foundational to cybersecurity? Foundational courses in this study are called Gateway courses.
2) Are there differences in availability by state, Title I status, size and locale?
3) How many courses are offered by type (Gateway, Non-Gateway, Cybersecurity)?

Attendance and Access

1) How many students attend the schools and CTE centers with gateway and cybersecurity courses?
2) Are there attendance differences by state?
3) Are there attendance differences by race/ethnicity?
4) Given availability levels along with other limitations (limited teachers, computer labs, and available hours), how many high school students have access to gateway computing and cybersecurity courses?
5) Are there differences in access by state?
6) Are there differences in access by student race/ethnicity? (Dark et al., 2020)

4. ARIZONA'S CYBERSUPPLY

Arizona's CyberSupply data collection project partnered with Dark Enterprises' personnel, who conducted the initial CyberSupply data collection in 2020. This partnership allowed researchers to leverage the original research methodology, align with research questions, and benefit from lessons learned and best practices. This project was sponsored by the Center for the Future of Arizona (CFA) in partnership with the University of Arizona during Fall 2023. CFA is a nonprofit, nonpartisan organization that provides education, workforce development, and civic engagement programming. Specifically, the Arizona Pathways to Prosperity (APTP) initiative creates "future opportunity and upward economic mobility for all young Arizonans while supporting state and regional talent needs" (Center for the Future of of Arizona [CFA], 2025). APTP develops career-connected pathways in critical career fields, like cybersecurity, to provide career exploration, early college programs of study, and work-based learning (CFA, 2025). In addition to identifying the availability, attendance, and access of gateway, non-gateway, and cybersecurity courses, Arizona's CyberSupply data collection project had the following additional goals:

1) Identify schools of opportunity to develop cybersecurity courses or programs.
2) Identify schools with cybersecurity courses or programs to articulate pathways to higher education.
3) Identify schools with cybersecurity courses or programs to provide career exploration and career readiness opportunities.

Methodology

As previously mentioned, a subset of the research questions outlined in the High School Designation Feasibility Study was used to develop the research questions for this study. The research questions are:

Availability

1) What percentage of schools and CTE centers have cybersecurity courses and computing courses that would be foundational to cybersecurity? Foundational courses in this study are called Gateway courses.
2) Are there differences in availability by size, Title I status, and locale?
3) How many courses are offered by type (Gateway, Non-Gateway, Cybersecurity)?

Attendance and Access

1) How many students attend the schools and CTE centers with gateway and cybersecurity courses?
2) Given availability levels along with other limitations (limited teachers, computer labs, and available hours), how many high school students have access to gateway computing and cybersecurity courses?

Although state-to-state comparison is briefly reviewed, it is important to note the timeframe between the original data collection and Arizona's data collection. The availability and access to cybersecurity courses in the original 11 states may have changed.

Purposive sampling was used during this study, which refers to a group of non-probability techniques in which units are selected because they have characteristics needed in the sample (Nikolopoulou, 2022). Purposive sampling is best suited to help answer the identified research questions, particularly when a lot of background information is available. Homogeneous sampling was used to reduce variation and simplify the analysis to describe a particular subgroup in depth.

Data Collection

Researchers from the University of Arizona (U of A) and undergraduate students from the U of A, Grand Canyon University (GCU), and Pima Community College (PCC) conducted data collection during the 2023-2024 academic year. Data sources included the Common Core of Data from the National Center for Education Statistics (NCES).

- Data on enrollment, race/ethnicity, free/reduced lunch, Title I status, size, and locale were gathered from NCES.
- Data on course availability were gathered from publicly available websites. Undergraduate students manually collected this data, which was then reviewed by faculty and personnel from Dark Enterprises to validate the findings.

Schools

Arizona's CyberSupply course availability data is reported for 349 schools identified in the final dataset with an estimated total population of 319,079 high school students. Most schools were considered "small schools" with less than 600 students (54.2%), Title I schools (54.4%), and located within a city (43.6%). The breakdown for each category is provided in Tables 2, 3, and 4.

School Size	f	%
<600 Students	189	54.2
600-1200 Students	44	12.6
1201-2000 Students	62	17.8
>2000 Students	54	15.5
Total	349	100.0

Table 2 – School Size

Title I	f	%
Yes	190	54.4
No	159	45.6
Total	349	100.0

Table 3 – Title I Schools

Locale	f	%
City	152	43.6
Suburb	70	20.1
Town	51	14.6
Rural	76	21.8
Total	349	100.0

Table 4 – School Locale

Courses

This study identified 667 computing and 73 cybersecurity courses, as outlined in Tables 5 and 6, respectively. Courses considered computer science gateway are annotated with (CSG), those considered IT gateway are annotated with (ITG), and non-gateway courses are annotated with (NG).

Pathway	Course	f	%
Computer Science Gateway	AP CSP / CSP	73	10.9
	AP CSA	56	8.4
	CS Discoveries	5	0.7
	CS Essentials	8	1.2
	Exploring CS	4	0.6
	Introduction to CS	50	7.5
	Linux	3	0.4
	Programming I	83	12.4
	Programming II	69	10.3
	Programming III	38	5.7
	Exploring CS	4	0.6
Information Technology Gateway	IT Fundamentals	41	6.1
	Networking I	15	2.2
	Networking II	11	1.6
	Networking III	4	0.6
Non-Gateway	Capstone Course I	47	7.0
	Capstone Course II	21	3.1
	Computer Applications	1	0.1
	Computer Management and Support	27	4.0
	Database	0	0
	Digital Media	11	1.6
	Game Design/ Development I	18	2.7
	Game Design /Development II	8	1.2
	Mobile App Design/ Development	10	1.5
	Robotics	33	4.9
	Web Design	20	3.0
	Web Design II	11	1.6
	Total	667	100

Table 5 – Computing Courses

Course	f	%
Intro to Cybersecurity	21	29
Cybersecurity II	17	23
Cybersecurity III	14	19
Principles of Cybersecurity	16	22
Network Security	0	0
Cyber Forensics	0	0
Cyber Ops	1	1
Advanced Cyber Forensics	0	0
Other	4	5
Total	73	100

Table 6 – Cybersecurity Courses

Analysis

The formula for calculating access (Figure 1) is the number of courses (C) multiplied by the number of available seats (P). 30 is used for available seats to align with the feasibility study. C x P is divided by the total number of students (T) divided by four (4) to determine the approximate number of students per grade (4)

$$A = \frac{C \times P}{T/4}$$

Figure 1 – Access Formula

Analysis of the data and available courses identified that 48% of schools provided gateway courses across 460 different courses (667 (total courses)-207 (NG-labeled courses) =460 different courses from Table 5). 70% of total students from the study have access to these courses, providing an estimated 34% access to gateway courses.

Additionally, 10% of schools provided cybersecurity courses across 73 courses. These schools accounted for 2% of total students, providing an estimated 2.7% access to cybersecurity courses. Further, <1% of students have access to a cybersecurity pathway. Pathways are career-themed and college preparatory programs in high schools and CTE centers. Cybersecurity is often found in either the IT or STEM career cluster.

Tables 7 through 15 provide a cross-tabulation of computing courses, gateway computing courses, and cybersecurity courses across school size, Title I status, and locale, respectively, and provide the following information. Profile information and key findings from this data are summarized below.

Profile of Schools and Students

- 78% of AZ public high schools are Urban and 88% of students attend Urban Schools
- 33% of schools have >1200 students and 75% of students attend these schools
- 54% of AZ public high schools have <600 students and 13% of students attend them
- 54% of high schools are Title I

Key Findings

- 40% of schools offering gateway courses are Urban; 8% are rural schools
- 9% of schools offering cyber courses are urban; 1% are rural schools
- 78% of schools with 1200+ students offer gateway courses; 15% offer cybersecurity courses
- 34% of schools with <1200 students offer gateway courses; 7% offer cybersecurity courses

	Computing Courses		
School Size	**Yes**	**No**	**Total**
<600 Students	68	121	189
600-1200 Students	29	15	44
1201-2000 Students	46	16	62
>2000 Students	45	9	54
Total	188	161	349

Table 7 – Computing Courses and School Size

	Gateway Computing		
School Size	**Yes**	**No**	**Total**
<600 Students	54	135	189
600-1200 Students	25	19	44
1201-2000 Students	45	17	62
>2000 Students	45	9	54
Total	169	180	349

Table 8 – Gateway Computing and School Size

	Cybersecurity Courses		
School Size	**Yes**	**No**	**Total**
<600 Students	12	177	189
600-1200 Students	5	39	44
1201-2000 Students	8	54	62
>2000 Students	9	45	54
Total	34	315	349

Table 9 – Cybersecurity Courses and School Size

	Computing Courses		
Title I	**Yes**	**No**	**Total**
Yes	96	94	190
No	92	67	159
Total	188	161	349

Table 10 – Computing Courses and Title I

	Gateway Computing		
Title I	**Yes**	**No**	**Total**
Yes	85	105	190
No	84	75	159
Total	169	180	349

Table 11 – Gateway Computing and Title I

	Cybersecurity Courses		
Title I	**Yes**	**No**	**Total**
Yes	19	171	190
No	15	144	159
Total	34	315	349

Table 12 – Cybersecurity Courses and Title I

	Computing Courses		
Locale	**Yes**	**No**	**Total**
City	86	66	152
Suburb	43	27	70
Town	24	27	51
Rural	35	41	76
Total	188	161	349

Table 13 – Computing Courses and Locale

	Gateway Computing		
Locale	**Yes**	**No**	**Total**
City	79	73	152
Suburb	43	27	70
Town	19	32	51
Rural	28	48	76
Total	169	180	349

Table 14 – Gateway Computing and Locale

	Cybersecurity Courses		
Locale	**Yes**	**No**	**Total**
City	22	130	152
Suburb	5	65	70
Town	4	47	51
Rural	3	73	76
Total	34	315	349

Table 15 – Cybersecurity Courses and Locale

Arizona's CyberSupply data was compiled into the dataset from other states. Figure 2 outlines the availability of Gateway Computing courses and Cybersecurity courses across 13 states. Figure 3 outlines the access to those courses across states. Several key takeaways are identified by viewing this consolidated data. First, there are prominent outliers in several states. For example, the availability of gateway computing courses in Maryland at 91% is contrasted with the relatively low access to those courses at 38%. Similarly, the availability of cybersecurity courses in Virginia at 61% contrasts with access being calculated at just 14%. Second, the average availability for Gateway Courses is 59% or 56% when removing the Maryland outlier. The average availability for Cybersecurity courses is 16% or 12% after removing the Virginia outlier. There are no significant outliers for Gateway access, resulting in an average access of 46% across states. However, when calculating access for cybersecurity, averages are considered with Virginia and without, resulting in 3.7% or 2.9%, respectively.

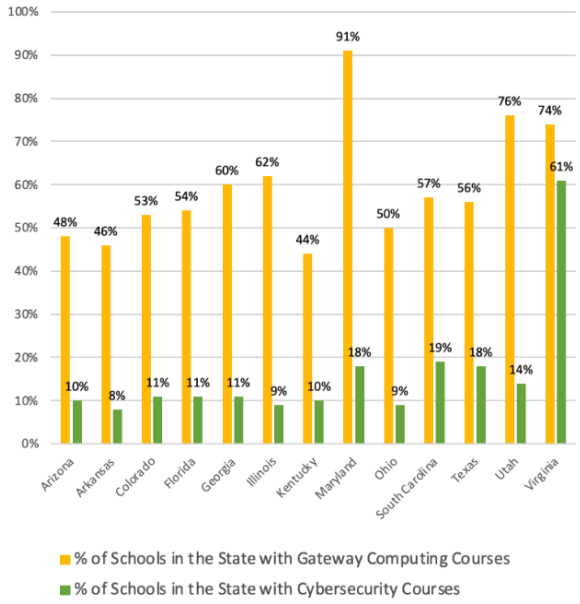


Figure 2 – Availability by State with Gateway Computing vs Cybersecurity Courses (Dark et al., 2020)

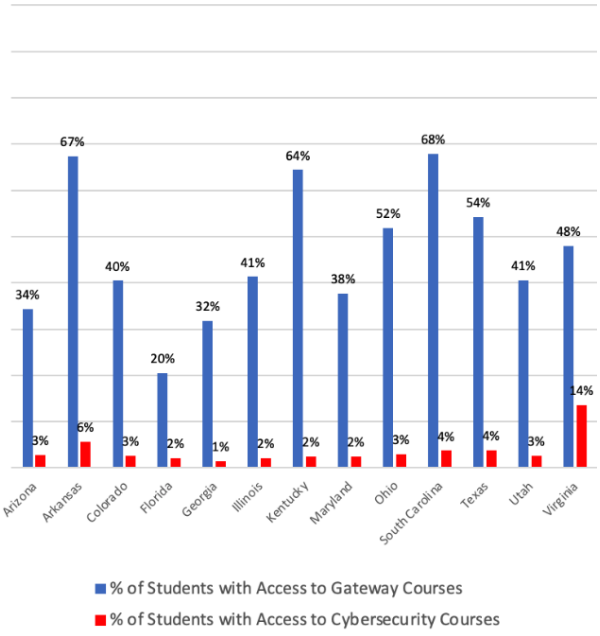


Figure 3 – Access by State with Gateway Computing vs Cybersecurity Courses (Dark et al., 2020)

Finally, researchers developed Figures 4 and 5 to highlight the side-by-side comparisons of availability and access from states included in this study. Figure 4 shows that in some instances (Arkansas, Kentucky, Ohio, and South Carolina), there is greater access to courses than availability. Alternatively, Figure 5 shows the differences between availability and access are proportionally similar except for Virginia.

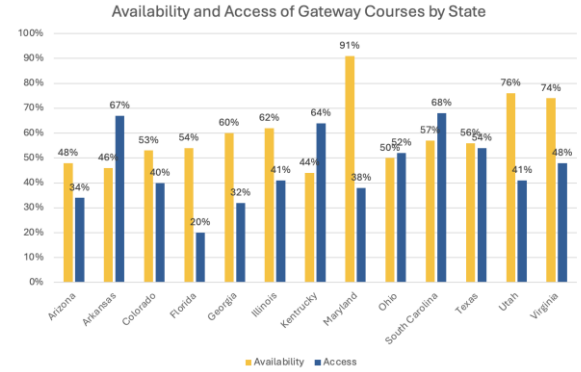


Figure 4 – Availability and Access of Gateway Courses by State

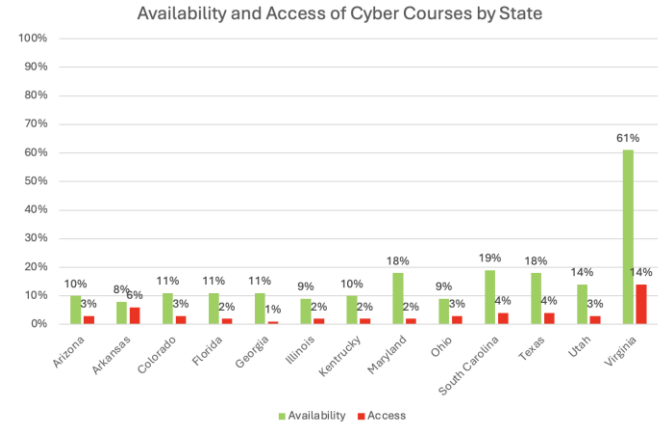


Figure 5 – Availability and Access of Cybersecurity Courses by State

5. FUTURE WORK

This study provides multiple possibilities for future work. Analysis of outlier states and those tat have more access to courses than availability could identify best practices, resources, or methods for developing and increasing the availability and access for gateway and cybersecurity courses within Arizona. Additionally, researchers noted a three to four-year gap between the original data collection and Arizona's data collection. Evaluating the ability to conduct regular data collection and expanding it to other states could further identify areas of opportunity and excellence to inform decision-making. This could also lead to year-over-year trend analysis to identify whether availability and access are increasing or decreasing. Further, researchers will leverage this data to identify schools for development, support, or expansion. It could identify why schools with low, or no availability are not offering gateway or

cybersecurity courses. Finally, this study provides information on schools with gateway and cybersecurity courses. This provides the opportunity to develop a community of practice and connection with schools to ensure districts, teachers, and programs are sustainable. This would enable the development and distribution of best practices, staying current with the evolving nature of cybersecurity, and conducting professional development. The community of practice can be facilitated through statewide initiatives, including GenCyber, Arizona Cybersecurity Initiative, the National Cybersecurity Teaching Academy (NCTA), Arizona Teaching Academy, and the 18-credit Graduate Certificate in Cyber Operations offered by the University of Arizona.

6. CONCLUSIONS

The availability and access to gateway and cybersecurity courses at secondary education institutions are critical to overcoming the cybersecurity skills and workforce shortage. Cybersecurity education at the high school level lacks availability and access, with only 10% of Arizona schools offering cybersecurity courses and less than 1% of students having access to cybersecurity pathways. Changing access in Arizona can occur in several ways. First, leveraging interest in computer science can develop interest in cybersecurity. Since 48% of schools offer gateway to cybersecurity courses it provides an opportunity to develop interest through those courses. Second, offering multiple entry points into cybersecurity pathways can be beneficial. Cybersecurity professionals have diverse backgrounds and enter the career field at different points. Cybersecurity education should provide similar opportunities and a diverse range of pathways. Additionally, states and schools need to invest in teachers and cybersecurity professional development. There are local and national training opportunities ranging from camps and professional development, like GenCyber and Cybersecurity High School Innovations (CHI), to scholarships for a graduate certificate in cybersecurity provided by the NCTA. Finally, Arizona needs to incentivize schools and districts to initiate and grow cybersecurity pathways. This may include implementing state standards and requirements for cybersecurity or developing a dedicated CTE program for cybersecurity.

Actions must be taken to address Arizona's and the nation's critical cybersecurity workforce shortage by expanding access and availability of cybersecurity education in our secondary schools. Educators, policymakers, and industry leaders should collaborate to leverage existing computer science programs, create diverse entry points into cybersecurity pathways, and invest in teacher training and professional development. By incentivizing schools and districts to build robust cybersecurity programs and adopting clear state standards, states can empower their students with the skills needed for tomorrow's digital challenges.

7. ACKNOWLEDGEMENTS

The Center for the Future of Arizona (CFA) provided funding for this research project. Their generosity and support for cybersecurity education are invaluable to Arizona students. Additionally, we appreciate the support of Dark Enterprises in conducting the data collection and analysis for this study.

8. REFERENCES

ABET. (2025). *About ABET.* https://www.abet.org/about-abet/

National Center for Education Statistics. (2025). *About NCES*. https://nces.ed.gov/about/

ABET. (2025). *Accredited programs*. https://amspub.abet.org/aps/category-search?disciplines=91&disciplines=94

Association for Computing Machinery (ACM), IEEE-CS, AIS SIGSEC, & IFIP WG 11.8. (2017). *Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity*. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

Becker, A., Blum, Z., Burgin, K., Carlin, A., Chu, B., Cranford-Wesley, D., Frank, S., Ghosh, T., Hamman, S., Joyce, R., Keller, S., Kohnke, A., Levy, Y., Liu, X., Manikas, T., McBride, S., Mierzwa, S., Miller, S., Nagaishi, M., Nowatkowski, M., Pinto, A., Steiner, S., Taylor, B., Tu, M., Weathers, R., West, T., & Zanella, G. (2024). *National Centers of Academic Excellence in Cybersecurity (NCAE-C) – Cyber Defense (CAE-CD) knowledge units (KUs)*. National Security Agency. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf

Center for the Future of Arizona (CFA). (2025). *Arizona pathways to prosperity*. https://www.arizonafuture.org/media/ok5pbis5/aptp-flier-statewide-v4.pdf

Cyber.org, Cyber Innovation Center, & Cybersecurity and Infrastructure Security Agency. (2021). *K-12 cybersecurity learning standards*. https://cyber.org/sites/default/files/2021-10/K-

12%20Cybersecurity%20Learning%20Standards_1.0.pdf

CyberSeek. (2025). *Cyberseek supply and demand heat map*. https://www.cyberseek.org/heatmap.html

Dark Enterprises. (2023). *Cybersecurity education: Availability and access in public high schools*. CyberSupply Securing the Workforce. https://cybersupply.org/

Dark, M., Daugherty, J., Williams, T., & Sands, J. (2020). *2020 NCAE-C high school designation feasibility study*. National Cryptologic Foundation. https://caecommunity.org/sites/default/files/initiatives/files/Feasability_Study_Final_NCAE-C_2020.pdf

ISACA. (2023). *State of cybersecurity 2023: Global update on workforce efforts, resources, and cyberoperations*. https://www.isaca.org/resources/reports/state-of-cybersecurity-2023

ISC2. (2023). *How the economy, skills gap, and artificial intelligence are challenging the global cybersecurity workforce*. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

Kwak, J. (2020, June). What are gateway courses and why do they matter to equity in higher ed? *Every Learner Everywhere*. https://www.everylearnereverywhere.org/blog/what-are-gateway-courses-and-why-do-they-matter-to-equity-in-higher-ed

Nikolopoulou, K. (2022, August 11). What is purposive sampling? Definition and examples. *Scribbr*. https://www.scribbr.com/methodology/purposive-sampling/

National Centers of Academic Excellence in Cybersecurity (NCAE-C). (2025). *CAE institution map*. https://www.caecommunity.org/cae-map

National Security Agency (NSA). (2025). *National centers of academic excellence in cybersecurity*. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

Ross, W., & Duke, E. (2018). *Supporting the growth and sustainment of the nation's cybersecurity workforce: Building the foundation for a more secure American future*. U.S. Department of Commerce & Department of Homeland Security. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/executive-order-13800/supporting-growth-and-sustainment

Teach Cyber & National Cryptologic Foundation. (2021). *High school cybersecurity curriculum guidelines & glossary*. https://teachcyber.org/wp-content/uploads/2022/11/High-School-Cybersecurity-Curriculum-Guidelines-Nov2022.pdf

White, A., & Bunce, J. (2023). *Generative AI and cybersecurity: Bright future or business battleground?* Sapio Research. https://www.deepinstinct.com/pdf/voice-of-secops-4th-edition

Linking Security Self-Efficacy and Communication Networks to Perceived Success in Cybersecurity Tabletop Exercises

Shawn F. Clouse
shawn.clouse@umontana.edu

Theresa Floyd
theresa.floyd@umontana.edu

College of Business
University of Montana
Missoula, MT 59812, USA

Ryan T. Wright
ryan.wright@virginia.edu
University of Virginia
Charlottesville, VA 22904, USA

Patricia Akello
patricia.akello@mso.umt.edu

Reda Haddouch
reda.haddouch@umontana.edu

College of Business
University of Montana
Missoula, MT 59812, USA

Abstract

This study examines a multi-organization Tabletop Exercise (TTX) involving state and national agencies to provide insights into how social cognition and network factors influence exercise outcomes. Building on Social Cognitive Theory and Social Network Theory, this study proposes a model linking psychological factors, such as self-efficacy, and communication network structures to participants' perceptions of organizational performance and training benefits. The research explores how communication networks and people's confidence in their organization's abilities affect participants' perceptions of the exercise's success. The study highlights the importance of security self-efficacy, demonstrating how beliefs in organizational capability influence engagement and perceived success. By connecting psychological readiness with network structures, this work advances a more comprehensive understanding of how to design, implement, and evaluate impactful cybersecurity TTXs, strengthening preparedness for complex, high-stakes cyber incidents. Findings underscore the critical role of communication structures: participants embedded in larger and more central networks reported higher assessments of their organization's performance and the exercise's value. Perceived security self-efficacy was a key factor for positive results. The findings recommend designing TTX for groups with different maturity levels and encouraging inclusive communication.

Keywords: Social networks, Cybersecurity tabletop exercises (TTXs), Critical infrastructure, Incident response.

Recommended Citation: Clouse, S.F., Floyd, T., Wright, R., Akello, P., Haddouch, R., (2026). Linking Security Self-Efficacy and Communication Networks to Perceived Success in Cybersecurity Tabletop Exercises. *Cybersecurity Pedagogy and Practice Journal;* v5(n1) pp 52-78. DOI# https://doi.org/10.62273/FYBR1844

Linking Security Self-Efficacy and Communication Networks to Perceived Success in Cybersecurity Tabletop Exercises

Shawn F. Clouse, Theresa Floyd, Ryan T. Wright, Patricia Akello and Reda Haddouch

1. INTRODUCTION

Cybersecurity professionals and government agencies have warned that the US power grid and critical infrastructure are vulnerable to devastating malicious attacks (Ling, 2025). As cyber threats to critical infrastructure continue to rise, organizations across both public and private sectors are turning to Tabletop Exercises (TTXs) as a key tool for cybersecurity and incident response preparedness. For example, "Operation 999" was a ransomware TTX focused on the water industry, which allowed participants an immersive experience to practice incident response strategies (Leyden, 2025). TTXs offer a low-cost, scenario-based method to simulate incident response and test decision-making, coordination, and communication strategies in a safe, controlled environment. They combine experiential learning with realistic scenarios to train organizational personnel effectively (Maurer, 2023). When implemented, these exercises significantly enhance both technical and essential soft skills, bridging gaps frequently observed among professionals and new graduates (Angafor et al., 2020). These exercises are especially valuable for improving not only technical readiness but also soft skills such as collaboration, leadership, and adaptability (Angafor et al., 2020; Pate et al., 2016).

Empirical evidence from healthcare, education, transportation, and the pharmacy sectors reinforces the effectiveness of TTXs, showing substantial improvements in knowledge, attitudes, confidence, and practical response capabilities compared to traditional lecture-based training (Brunner & Lewis, 2006; Mirzaei et al., 2020; Pate et al., 2016; Radow, 2007). Businesses frequently rely on TTX for their cybersecurity training and preparedness needs (Pearlson et al., 2021). Further, CISA, the U.S. government organization charged with protecting national cybersecurity and infrastructure from cyber threats, actively endorses this training method by providing ready-made TTX packages, reflecting their advocacy as a standard practice (*Cybersecurity & Infrastructure Security Agency*, 2025). Moreover, the National Institute for Standards and Technology (NIST) has put TTX as a common and valuable practice in their NIST Cybersecurity Framework (CSF) to help organizations test and improve their response capabilities (National Institute of Standards and Technology, 2024). In summary, Tabletop exercises (TTXs) are widely used for emergency preparedness by several disciplines, including Cybersecurity, and much work has gone into the design of these programs, yet effective Cybersecurity TTX implementation is not as well understood (Haddouch et al., 2025).

Although TTXs are widely used, their effectiveness is not completely clear and they tend to be assessed differently based on the situation. This study addresses this gap by integrating a social-cognitive perspective with a social network lens to explain why some exercises yield stronger perceptions of value and performance than others. This research argues that participants' self-efficacy and perceptions of collective capability shape how they engage during the exercise, and these engagement processes, in turn, influence what participants believe they gain from the experience.

At the same time, these cognitive mechanisms are conditioned by the structure of communication and collaboration during the TTX: who interacts with whom, how centralized or fragmented the interaction patterns are, and whether participants occupy bridging or peripheral positions. By examining cognition and network structure jointly, the research moves beyond "did the exercise work?" to specify how and under what social conditions TTXs produce more meaningful learning, coordination, and preparedness outcomes, especially in cross-functional and cross-organizational settings where TTXs are most often deployed.

The goal of TTX is to assess an organization's preparedness and response capabilities for various scenarios by simulating real-world situations in a low-risk, discussion-based environment (Cybersecurity & Infrastructure Security Agency, 2025). A key outcome is developing and testing coordination and communication(Everbridge, 2025; Haddouch et al., 2025). In a literature review, Vykopal et al. identified 140 research papers explicitly

examining TTXs. "Out of only three papers (P4, P6, and P8) that addressed assessment, only one (P6) suggested a method that goes further than unstructured assessment by the observers and facilitators" (Vykopal et al., 2024, p. 223). There is an opportunity to provide a theoretically driven, rigorous assessment of the outcomes of the TTX beyond observational data.

This study focuses on evaluating participants' perceptions of their organization's performance and the benefits gained from a TTX situated in the context of critical infrastructure protection in rural areas, where resource constraints and unique communication challenges make effective team coordination and training implementation particularly important. This research examines the impact of a key learning factor drawn from social cognitive theory (Bandura, 1997), in concert with factors related to the network of interactions between participants to better understand how to effectively implement and evaluate TTXs in cybersecurity and beyond. This research identifies key psychological and contextual factors—such as self-efficacy (belief in one's ability to accomplish a specific task), network size, and network centrality (one's structural position within a network)—that are often overlooked in traditional linear TTX evaluations. Thus, this study supports the development of a research model that explains how these factors shape perceived performance and benefits during TTXs, particularly in resource-constrained environments like rural infrastructure settings. By connecting psychological readiness and social networks, this research offers a more comprehensive understanding of how to implement and evaluate impactful TTXs in cybersecurity and beyond.

2. LITERATURE REVIEW & THEORETICAL FOUNDATION

Tabletop exercises: Design, efficacy, and evaluation gaps

Tabletop exercises (TTXs) are becoming more common in critical infrastructure industries, allowing organizations to practice responding to cyber threats in a safe, low risk setting. Additionally, TTXs have emerged as an effective method for enabling participants to collaboratively address complex cybersecurity incidents affecting critical infrastructure. According to Evans (2019), such scenarios provide a low-stress yet high-impact setting that enables participants to enhance their comprehension of cyber threats while improving their collaborative, communicative, and decision-making abilities in simulated real-world conditions (Evans, 2019). In complex scenarios, the integration of public-private partnerships and civilian-military collaboration becomes essential.

As Elvegård and Andreassen (2024) emphasize, TTXs facilitate interagency coordination by engaging multiple organizations, thereby enhancing mutual recognition of cyber risks and increasing awareness of shared resources and response capabilities (Elvegård & Andreassen, 2024). Maennel et al. (2023) stress the necessity of joint efforts across sectors to develop comprehensive cyber-defense mechanisms capable of addressing large-scale, multifaceted security incidents. The inclusion of diverse disciplinary perspectives and varying levels of expertise within these exercises further enriches the collective problem-solving process.

A critical element of interagency collaboration is establishing a clear understanding of roles and shared expectations during cybersecurity incidents. In alignment with these principles, the NIST 800-84 guidelines (Grance et al., 2006) endorse TTXs as a key component within broader test, training, and exercise (TT&E) programs aimed at strengthening preparedness for cybersecurity events. Organizations should adopt best practices for TTXs to be prepared to address security events.

Bartnes and Moe (2017) identify several critical success factors in the design and execution of TTXs, including clearly defined objectives, time-sensitive decision points, realistic role assignments, and active involvement of key stakeholders. When these elements are met, TTXs have the potential to enhance both technical competencies and non-technical skills, such as leadership and collaboration (White et al., 2004; Young & Farshadkhah, 2022). Despite their recognized value, much of the existing literature primarily assesses TTXs through the lens of compliance and organizational readiness benchmarks. Less attention has been paid to the interpersonal and structural dynamics that shape the efficacy of these exercises.

Tobergte et al. (2022) argue that the most impactful TTXs are those that replicate authentic cognitive and emotional stressors, mirroring the uncertainty and complexity of real-world incidents. Nonetheless, empirical investigations into interactional patterns—such as communication flows, centrality in problem-solving networks, and their influence on learning outcomes remains limited. The current study seeks to fill this gap by examining the relational and organizational conditions that optimize learning and coordination in cybersecurity tabletop exercises.

Social Cognitive Theory

Social Cognitive Theory (SCT) posits that individuals' beliefs about their capabilities influence their behavior, motivation, and outcomes (Bandura, 1977, 1997). When extended to the group or organizational level, collective efficacy reflects the shared belief that the team or organization is capable of successfully performing a given task. In the cybersecurity context, this theoretical lens has proven powerful in explaining behavioral variation in both proactive and reactive security behaviors.

A landmark early application of this theory in the information systems domain is found in Compeau and Higgins (1995). In the study, Compeau and Higgins (1995) developed and validated a scale for computer self-efficacy (CSE) and demonstrated its predictive power for individual computer usage behavior, beyond actual skill level. CSE was updated in 2022 to IT self-efficacy (ITSE) as CSE has a narrow desktop-centric view of computing, which does not translate to the platform and mobile environment of today. ITSE acknowledges that confidence in using IT now extends to environments where users may interact with systems indirectly (e.g., voice interfaces, AI tools) or rely on highly automated systems (D. Compeau et al., 2022). Extending this to the cybersecurity domain, Johnston and Warkentin (2010) applied self-efficacy theory to model end-user compliance with security policies. The study empirically tested the role of self-efficacy alongside fear-based appeals in shaping users' security behavior intentions, finding that users who believed in their ability to enact secure behaviors were significantly more likely to avoid risky actions such as opening phishing emails or using weak passwords (Johnston & Warkentin, 2010). Further, Stavrou and Piki (2024) found that cultivating self-efficacy is a key attribute in developing cybersecurity skills. These findings highlight the importance of psychological readiness in shaping security-related performance.

Similarly, Ifinedo (2012) used social cognitive theory to explore employee compliance intentions within organizations. The study advanced a model that integrates self-efficacy within a broader behavioral framework, combining the Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT) to examine what drives user compliance with security policies. His findings demonstrate that self-efficacy, perceived behavioral control, and response efficacy are key predictors of intention to comply with security policies. This work is particularly relevant in organizational contexts where employee awareness, confidence, and perceived capability significantly influence security posture (Ifinedo, 2012). In the context of cyber team readiness, Durcikova et al. (2024) empirically examined how organizational cybersecurity self-efficacy relates to real-world breach outcomes, reinforcing the view that collective belief systems or organizational security self-efficacy are predictive of performance in high-uncertainty, high-stakes environments like cybersecurity (Durcikova et al., 2024). In sum, there is clear evidence that social cognition plays an important role in technology interactions and decision making, which are both critical in TTXs.

Social Network Theory

While social cognitive theory explains why individuals and teams may engage in effective behavior during TTXs, Social Network Theory helps explain how those behaviors unfold across communication structures. Social Network Theory conceptualizes social systems as sets of nodes (people) and ties (interactions), and emphasizes how structural position within a network affects access to resources, influence, and information (Borgatti & Li, 2009; Burt, 1992; Freeman, 1978). Two constructs—network size and centrality—are relevant in time-sensitive, collaborative environments like TTXs. In an early application of social network theory to organizational behavior, Brass (1984) conducted a study on organizational influence, revealing that individuals with high centrality in communication networks wield significant informal power, often surpassing those with formal authority. The study found that structural position within a network, i.e., centrality, is an important predictor of influence over decision-making and performance outcomes (Brass, 1984). This principle was extended to emergency management and security contexts by Monge & Contractor (2003), who extended Social Network Theory into high-pressure organizational environments, demonstrating that communication structure, not just technical expertise, plays a decisive role in determining team effectiveness during complex coordination tasks. Their work underscores the predictive value of network properties such as density and connectivity for group performance (Monge & Contractor, 2003).

In the cybersecurity space, Gordon et al. (2003) argued for the importance of inter-organizational information sharing in preventing security breaches and proposed early models of collaborative security readiness. The authors emphasized that timely and strategic information flow between networked actors is essential for preempting and mitigating security breaches, shifting the focus from isolated technical controls to collaborative readiness (Gordon et al., 2003).

A study examining cybersecurity skills, specifically phishing detection within organizations, found that an individual's centrality within a department, as determined by social network analysis, is associated with cybersecurity compliance (Wright et al., 2023). In addition, this study found that IT self-efficacy was identified as another factor related to cybersecurity skills and compliance. Similarly, Carley (2003, 2020) introduced the concept of social cybersecurity, applying computational network analysis to assess how information spreads through human networks and how trust and influence can be compromised. Her work highlights the importance of modeling not just who participates in exercises, but who connects, influences, and facilitates coordination; ideas that this study seeks to test in an applied TTX setting (Carley, 2003, 2020). Individual interactions and relationships, as assessed by a social analytics lens, are interconnected in significant situations and can influence outcomes. The authors believe this may be true in TTX as well.

To summarize this literature review, first, tabletop exercises (TTXs) are widely used and effective for improving preparedness, coordination, and both technical and non-technical skills across critical infrastructure sectors. Gross and Ho (2021) stated that experiential, team-based learning activities in cybersecurity enhance technical understanding, collaboration, and readiness for defensive tasks, supporting the value of exercises like TTXs. The literature review also indicates that existing studies primarily focus on exercise design, compliance, and organizational readiness, while giving limited attention to the social and structural processes that shape exercise outcomes. The literature on Social Cognitive Theory and Social Network Theory highlights that participants' beliefs about their organization's capabilities and the structure of in-exercise communication networks may play a critical role in determining perceived performance and training benefits. However, these factors have rarely been examined together in cybersecurity TTXs. This study addresses this gap by examining how perceived organizational security self-efficacy and communication network structure jointly influence exercise outcomes.

Research hypotheses

Building upon Social Cognitive Theory and Social Network Theory, this study advances a theoretically grounded model to explain how perceived organizational security efficacy and communication network structure may influence participants' perceptions of organizational performance and training benefit in cybersecurity Tabletop Exercises (TTXs). The hypotheses center around psychological antecedents (self-efficacy), structural mediators (network position), and the exercise-level outcomes (perceived performance and benefit).

Perceived security self-efficacy

Grounded in Social Cognitive Theory, perceived self-efficacy in the context of TTX refers to an individual's belief in their team or organization's ability to effectively respond to cyber threats. This belief serves as a motivational driver, influencing how participants approach engagement with team members and respond to simulated stress scenarios during the exercise.

Past research has long established the positive influence of self-efficacy across various domains (Bandura, 1997; Staples et al., 1999). At the team level, cybersecurity-specific self-efficacy reflects the collective confidence of a group in executing cyber incident response tasks (Judge & Bono, 2001). Recent empirical work also reinforces this view. Durcikova et al. (2024) investigated how collective self-efficacy within cybersecurity teams affects an organization's resilience against breaches . The study found that high team efficacy led to fewer and less severe security incidents, emphasizing that belief in competence influences not just individual behavior but also organizational vigilance and cohesion. Similarly, Park and Shin (2022) applied social cognitive theory to explore how group-level efficacy shaped team coordination during security-critical tasks, finding that overconfidence can sometimes degrade performance unless coupled with strong communication and accountability mechanisms. These findings align with the broader theoretical expectation that groups with elevated levels of self-efficacy and trust in their organization tend to exhibit better performance outcomes (Park & Shin, 2022; Ter Huurne & Gutteling, 2009).

These psychological factors are not only critical for performance but also shape interpersonal dynamics during TTXs. Specifically, higher levels of self-efficacy may lead participants to contribute more actively to group dialogue during the exercise, express concerns, and initiate communication more freely. These behaviors, in turn, influence the structure and quality of communication networks that form during the exercise, including participants' connectedness and central roles within those networks. It is acknowledged that individual attitudes and social network characteristics are posited to co-evolve over time, especially within organizational settings (Tasselli et al., 2015); however, because the in-exercise network formed during the

exercise, influenced only by the temporary teams that participants were assigned to, it is reasonable to assume that individual participants' pre-conceived notions of their organizations' security self-efficacy were unlikely to be influenced by the nascent network that emerged during the exercise, and instead were more likely to influence participants' behavior during the exercise, in turn affecting their network size and position.

Within the TTX environment, this research posits that heightened perceived security self-efficacy enables teams to more efficiently access and disseminate critical information, facilitating quicker and more effective connections to relevant actors and knowledge. Therefore:

H1: Perceived organizational security *self-efficacy is positively related to in-exercise communication network (a) size and (b) centrality.*

In-exercise communication networks

While individual-level beliefs serve as behavioral antecedents, the structure of communication during a TTX also plays an important role in shaping outcomes. Drawing from Social Network Theory (Borgatti et al., 2009; Freeman, 1978), this study examines two network-level constructs: a) network size and b) network centrality. These metrics capture the relational architecture of a TTX and are central to understanding how influence, coordination, and information flow unfold in real time.

The social network perspective conceives of the interconnected relationships and interactions between individuals as an informal structure that provides opportunities and imposes constraints (Borgatti et al., 2009). By examining the informal structure of the participants' communication during the exercise, the researchers explore how the relational context influences participants' access to information, ability to share information, and their influence on others, thus providing a deeper understanding of the factors affecting their perceptions of their organization's performance and the benefits of the exercise.

Network size is defined by the number of people each participant identified as effective communicators during the exercise (Freeman, 1978). Larger networks are associated with greater access to information and resources (Borgatti et al., 2009). Network centrality can be defined in several different ways. This study used *closeness network centralit*y (Freeman, 1978; Valente & Foreman, 1998), which is defined by the number of links it takes for each participant to reach all the other participants through the network. This concept of centrality is associated with independent access to information (because one has many potential contacts from which to gather information) and through this access, increased influence over others (Brass, 1984). Accordingly, in organizational crisis response, actors who are more central or better connected are often more influential in steering team decisions and synthesizing intelligence (Brilingaitė et al., 2022).

Therefore, the study expects that participants whose in-exercise communication networks are larger and whose positions within the networks are more central will evaluate their organization's performance in the exercise more favorably and will more highly rate the benefits of the exercise to their organization.

H2: In-exercise communication network size is positively related to a) perceived organizational performance in the TTX and b) perceived benefits of the TTX.

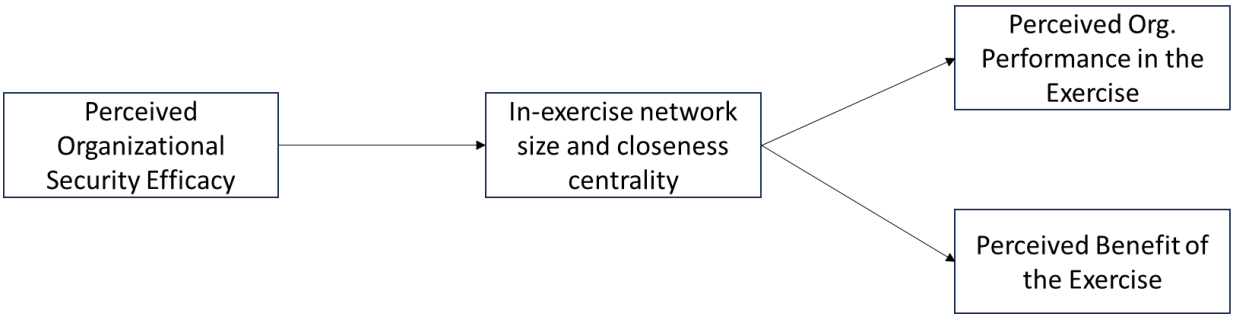
H3: In-exercise communication network centrality is positively related to a) perceived performance in the TTX and b) perceived benefits of the TTX.

Further, this research expects that in the high information velocity context of the TTX, where access to and control of information is highly important, a participant's network size and centrality will mediate the relationship between self-efficacy and the outcomes.

H4: In-exercise communication network size will mediate the relationship between perceived organizational security efficacy and a) perceived organizational performance and b) perceived benefits of the TTX.

H5: In-exercise communication network centrality will mediate the relationship between perceived organizational security efficacy and a) perceived organizational performance and b) perceived benefits of the TTX.

Figure 1. Integrated Model Based on Social Cognitive Theory and Social Network Theory.



Research model

Figure 1 illustrates the conceptual model that represents these hypotheses. The model integrates psychological beliefs (self-efficacy), communication structure (network size and centrality), and perceived outcomes (performance and benefit), providing a theory-driven explanation for variability in TTX effectiveness. In the proposed model, participants with higher perceptions of organizational security efficacy will have larger in-exercise communication networks and will be more central in those networks. In turn, in-exercise network size and centrality will influence participants' perceptions of their organizations' performance in the exercise and the benefits of the exercise for their organizations. Additionally, this research expects that in certain high-information velocity environments (e.g., TTX), where access to and control of information is highly important, the properties of a participant's in-exercise communication network (e.g., size and centrality) will mediate the relationship between self-efficacy and the outcomes.

3. METHODS

Study setting and TTX description

The study was situated in the context of critical infrastructure protection in rural areas, where resource constraints and unique communication challenges make effective team coordination and training implementation particularly important. The TTX took place in a rural state located in the Rocky Mountain West and focused on the electrical industry.

The TTX session started with an interdisciplinary planning team that organized the event and developed the exercise. The planning team included staff from the state's flagship university, staff from the Cybersecurity and Infrastructure Security Agency (CISA), staff from the state conducting the TTX training, and members from the critical infrastructure organizations. The planning team met several months prior to the event to develop goals for the TTX, develop the participant list, design the scenario for the exercise, and devise a plan to identify gaps during the after-action review. This exercise used the DECIDE Platform from Norwich University Applied Research Institutes (*NUARI*, n.d.) as a decision support system to be used during the exercise. DECIDE was developed with funding from the Department of Homeland Security, and it has been a trusted cybersecurity live exercise solution. The platform simulates cyber-attacks for organizations and their partners to stress and test incident response plans, resulting in after-action reports to improve strategic communication, compliance, risk, and overall resilience. The platform launches the different stages of the scenario in an email inbox interface. Participants can respond via a chat tool and there is a survey tool to capture qualitative and quantitative responses for each step of the TTX.

This exercise was designed to practice coordination, communication, and information sharing protocols between electric grid partner organizations while responding to a hypothetical disruptive cyber and physical incident. The integration of government, industry, military, and academia provides a strategic opportunity to work toward informed state-wide solutions with a robust network of partners. The participants in the exercise included employees from the public power company, 20 energy cooperatives, the Electric Cooperatives' Association, the state fusion center, the state Cybersecurity and Infrastructure Security Agency (CISA) representatives, National Guard, and state IT.

Procedure and participants

The event was held for six hours in two adjoining rooms at a large northwestern university. There were 25 players from the power industry and 21 players from state and federal agencies as well as the National Guard. Most of the participants (43) attended in person, and three attended virtually

via an internet video conferencing system (Zoom). All participants used laptops that were connected to the NUARI DECIDE Platform. All players, observers/scribes, and facilitators received DECIDE training prior to the TTX. NUARI provided staff to troubleshoot problems and to advance the injections for the exercise. Appendix 1 provides details about the exercise scenario. The in-person participants were assigned to eight groups distributed between two rooms at the facility; virtual participants were assigned to a ninth group. Each group included managers and technical staff from a power company or cooperative, as well as a National Guard representative.

There were facilitators for each step of the exercise as well as a facilitator for the virtual group. The facilitators roamed around to make sure each group was making progress on the discussion. There were 26 scribes who took notes on the discussions of the nine groups over the four modules of the TTX. The scribes all signed a Non-Disclosure Agreement, agreeing to keep the names of the participants and the organizations confidential. Their notes were submitted on the DECIDE Platform as a chat message. The facilitators explained each stage of the scenario, and then gave the participant teams 20 minutes to discuss. Then everyone was brought back together for a 15-minute large group discussion following each step of the TTX. During the 20-minute team discussions, few players entered comments into the DECIDE platform, so the content of the discussion was primarily captured by the scribes in DECIDE. The large group discussion was broadcast between the two rooms of the facility and to the virtual participants via Zoom. Prior to launching the next stage of the exercise, participants were given five minutes to respond to open-ended and Likert questions on the DECIDE Platform.

Survey instruments, measures, and analysis

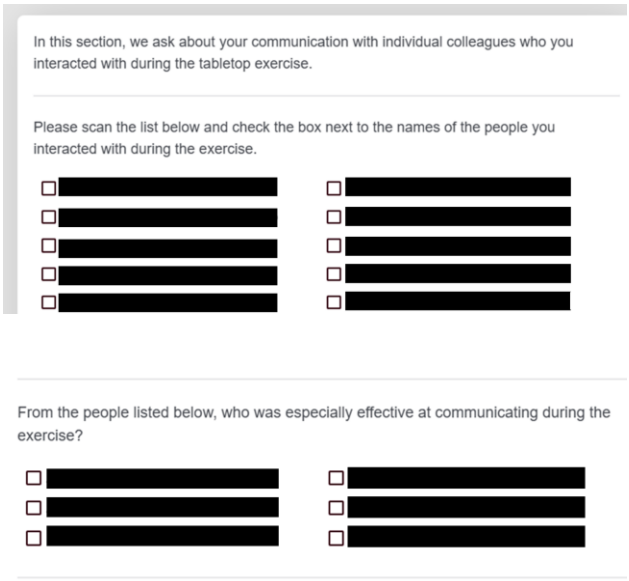
Online surveys were distributed via the DECIDE platform as well as via Qualtrics survey software (Qualtrics, Provo, UT). The research design included a pre-test survey administered before the participants began the exercise to elicit their organizational security efficacy, organization information, and demographics, and a post-test survey administered after participants completed the exercise to elicit their in-exercise networks, ratings of their organization's performance during the exercise, and their ratings of the benefits of the exercise for their organization. Both survey invitations were emailed to participants. The pre-test survey took about 10 minutes, and the post-test about 20 minutes. The data collected on Qualtrics was stored on a separate protected server, which only the researchers had access to. The Qualtrics surveys were encrypted using SSL security. Of the 46 participants, 39 completed both surveys (84.8% response rate).

Respondents were assigned a random ID code by the survey software. The investigators maintained one roster file containing participants' names and ID codes. This roster file was password protected and only accessed by the researchers. All analysis was done with the random ID code to protect the identity of the participants. The network map about who interacted with whom during the exercise is non-sensitive data that the organizations will use only to aid in future incident response planning. All participants were entered into a drawing for gift cards that were given out at the end of the TTX event. Participants could complete the survey only once, so incentives did not influence participation beyond survey completion.

Outcome and social cognitive variables were measured using Likert-type scales where 1= strongly disagree and 7= strongly agree. A complete list of survey items and confirmatory factor analyses is shown in Appendix 2. *Perceived organizational performance* in the exercise was measured using a 6-item scale adapted from Park & Shin (2022) and Cammann et el. (1979). Sample item: "Our organization exceeded its objectives for dealing with this cyber incident." *Perceived benefit of the exercise* was measured using a 3-item scale developed by (Wu & Wang, 2006) Sample item: "The tabletop exercise will benefit my organization." *Perceived organizational security efficacy* was measured using a three-item scale developed by Park & Shin (2022) and Cammann et al. (1979). Sample item: "My organization has above-average ability in responding to cybersecurity events."

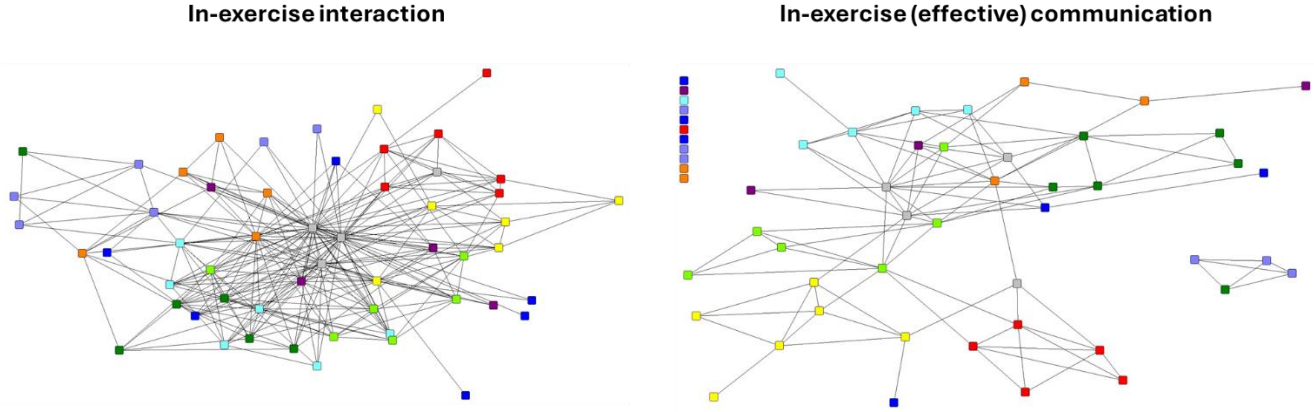
The in-exercise social networks were elicited using one-items measures, as is common in social network research (Marsden, 1990). First, participants were presented with a complete roster of all 46 participants and their organizational affiliations and asked to identify everyone they interacted with during the exercise. Next, participants were presented with a list of the participants they indicated that they interacted with and asked to identify which of those participants were especially effective at communicating during the exercise. Figure 2 displays the two social network questions, with participant names and affiliations redacted to maintain confidentiality.

Figure 2. Survey Items Used to Elicit In-exercise Interaction and Communication Networks



The resulting networks were thus 39 x 39 binary matrices, where a 1 in cell $x_{i,j}$ indicated that participant *i* identified *j* as an interaction partner or effective communicator. The networks were symmetrized using the maximum method, such that x_{ij} and x_{ji} were replaced by $\max(x_{ij}, x_{ji})$, i<j. i.e., if either member of the pair named the other, the tie was counted (Borgatti et al., 2024). This research chose the maximum method for symmetrizing the networks to capture the broadest possible network in each case and correct for any forgetfulness on the part of participants, since individuals have been found to be better at remembering long-term relationships than discrete instances of communication (Freeman et al., 1987). This research expects that effective communication benefits not only the effective communicators, but also the people they communicate with, so accounting for both incoming and out-going ties ensures that this research captures the full effect of the networks on the research outcomes. Communication network variables were calculated using UCINET VI (Borgatti et al., 2002). *Network size* was calculated using degree, a count of the number of people in each participant's communication network (Freeman et al., 1987). *Network closeness centrality* was calculated using

Figure 3. In-exercise Interaction and Communication Networks.



Average Reciprocal Distance (ARD) (Valente & Foreman, 1998), was calculated using the formula

$$C(i) = \frac{n-1}{\sum_{j=1}^{n-1} d(i,j)}$$

Where C(*i*) equals the closeness centrality for node *i*, *n* is the total number of nodes in the network, and d(*i,j*) is the geodesic distance of the shortest path between *i* and *j*, thus indicating the extent to which each participant had access to many effective communicators during the exercise.

This study tested several potential control variables, including age, race, gender, organizational affiliation, rank, position tenure, veteran status, organization size, number of employees in the organization's cyber unit, and number of cyber breaches. Only organization size and number of cybersecurity employees were significantly related to the outcome variables, so

all other controls were deleted for the sake of parsimony. Frequencies for categorical control variables are available in Appendix 3.

4. RESULTS

Refer to Figure 1 for the theoretical model, which outlines the hypothesized relationships between organization security self-efficacy, in-exercise communication network size and centrality, and perceived performance during the exercise and the benefit of the exercise. The sample size is insufficient for structural equation modeling (Wolf et al., 2013); thus, the authors used ordinary least squares (OLS) regression analyses to test for direct relationships and the PROCESS macro (Hayes, 2012) in IBM SPSS Statistics (version 29) for the path analysis of the mediation model. Indirect effects were tested using 5,000 bias-corrected bootstrap samples (Preacher & Hayes, 2008).

Network maps

Figure 2 presents the maps of the in-exercise interaction and communication networks. Nodes are colored according to group membership, with gray nodes indicating facilitators. Recall that the communication network identifies especially effective communication ties, so the communication network is sparser than the general interaction network.

Descriptives and zero-order correlations

Table 1 presents descriptive statistics and zero-order correlations. The relatively high means for perceived organization performance (5.52 out of 7) and benefit of the exercise (6.14 out of 7) indicate that participants generally thought their organizations had performed well and saw value in the exercise. Pre-exercise perceptions of organizational security efficacy were also relatively high (5.21 out of 7), indicating that participants generally believed that their organizations were competent to deal with cybersecurity incidents.

Table 1. Descriptive Statistics and Zero-order Correlations.

Variable	*N*	*Mean*	*SD*	*Min*	*Max*	1	2	3	4	5	6
1 Perceived organizational performance	39	5.52	0.87	3.00	7.00						
2 Perceived benefit of the exercise	39	6.14	0.83	4.00	7.00	.57**					
3 Perceived organizational security efficacy	43	5.21	1.61	2.00	7.00	0.29	-0.10				
4 In-exercise communication network size	55	3.67	2.98	0.00	13.00	.43**	0.32	0.22			
5 In-exercise communication network centrality	55	12.47	7.73	0.00	24.00	.33*	0.27	.33*	.83**		
6 Number of cyber professionals in organization	39	94.10	359.35	0.00	2000.00	-0.31	-0.29	0.30	0.25	0.16	
7 Number of employees in organization	39	1019.44	2806.18	8.00	17000.00	0.05	-.45**	0.11	0.15	0.12	0.46

Note. Table presents bivariate correlations. N=39
* $p < .05$. ** $p < .01$.

Model testing

Results of OLS regression analysis predicting communication network size and centrality are presented in Table 2. In Model 1, it was found that perceived organizational security efficacy is not significantly related to communication network size. In Model 2, it was found that security efficacy is positively and significantly related to communication network centrality. Thus, Hypothesis 1a is not supported and 2a is supported.

Results of OLS regression analysis predicting perceived organizational performance in the exercise are presented in Table 3. The control variable, number of cybersecurity professionals, was entered in Model 1, and was negatively and significantly related to perceived performance. Perceived organizational security efficacy, entered in Model 2, was positively and significantly related to perceived performance. The effect size and significance of this relationship are attenuated in the presence of the social network measures, providing some evidence of mediation. Communication network size and centrality were entered separately in Models 3 and 4 to correctly test the effects of each variable because social network variables, while theoretically distinct, are often empirically correlated. Both network measures are positively and significantly related to perceived performance, providing support for Hypotheses 2a and 3a.

Results of OLS regression analysis predicting perceived benefit of the exercise are presented in Table 4. The control variable, organization size (number of employees), was entered in Model 1, and was negatively and significantly related to perceived benefit. Perceived organizational security efficacy, entered in Model 2, is not significantly related to perceived benefit. Both

network variables are positively related to the outcome, providing support for Hypotheses 2b and 3b. Since perceived organizational security efficacy is not significantly related to perceived benefit, there is no evidence suggesting mediation, providing no support for Hypotheses 4b or 5b.

Table 2. Results of OLS Regression Analysis Predicting Communication Network Size and Centrality.

	Model 1 Network Size B *(SE)*	Model 2 Network Centrality B *(SE)*
Perceived organizational security efficacy	.39 (.27)	1.41* (.62)
Model F	2.08	5.14*
R2	0.05	0.11
Adjusted R2	0.03	0.09

$N = 39$. † $p < .10$ * $p < .05$ ** $p < .01$ *** $p < .001$.

Table 3. Results of OLS Regression Analysis Predicting Perceived Organizational Performance in Tabletop Exercise.

	Model 1 β *(SE)*	Model 2 β *(SE)*	Model 3 β *(SE)*	Model 4 β *(SE)*
Number of cybersecurity professionals in organization	-.31† (.00)	-.43* (.00)	-.53*** (.00)	-.48** (.00)
Perceived organizational security efficacy		.36* (.08)	.27† (.07)	.26 (.08)
In-exercise communication network size			.53*** (.04)	
In-exercise communication network centrality				.35* (.02)
Model F	3.79†	4.69*	9.94***	5.30**
R2	0.10	0.22	0.48	0.33
Change in R2		0.12	0.26	0.11
Adjusted R2	0.07	0.17	0.43	0.26

$N = 39$. † $p < .10$ * $p < .05$ ** $p < .01$ *** $p < .001$.

Table 4. Results of OLS Regression Analysis Predicting Perceived Benefit of Tabletop Exercise.

	Model 1 β *(SE)*	Model 2 β *(SE)*	Model 3 β *(SE)*	Model 4 β *(SE)*
Number of employees in organization	-.45** (00)	-43** (.00)	-.48** (.00)	-.46** (.00)
Perceived organizational security efficacy		-.11 (.08)	-.21 (.07)	-.24 (.08)
In-exercise communication network size			.44** (.04)	
In-exercise communication network centrality				.40* (.02)
Model F	8.65**	4.55*	7.13***	5.99**
R2	0.20	0.21	0.39	0.35
Change in R2		0.01	0.18	0.14
Adjusted R2	0.18	0.17	0.34	0.29

$N = 39$. † $p < .10$ * $p < .05$ ** $p < .01$ *** $p < .001$.

Table 5. Simple Mediation PROCESS Models Examining the Effect of Organizational Security Efficacy on Organizational Performance Through In-Exercise Communication Network Size and Centrality.

	Model 1 Mediating variable Network size β *(SE)*	Model 2 Mediating variable Network centrality β *(SE)*	Model 3 Dependent variable Perceived Performance β *(SE)*	Model 4 Dependent variable Perceived Performance β *(SE)*
Independent variables				
Number of cybersecurity professionals in organization	.00 (.00)	.00 (.00)	-.00*** (.00)	-.00** (.03)
Perceived organizational security efficacy	.30 (.30)	1.15† (.68)	.14† (.07)	.14 (.08)
Mediator variables				
In-exercise communication network size			.16*** (.04)	
In-exercise communication network centrality				.04* (.02)
Mediation (indirect effests)			Effect [95% CI]	Effect [95% CI]
Security efficacy ->Network size ->Performance			.05 [-.04, .13]	
Security efficacy ->Network centrality ->Performance				.05 [-.00, .17]
Constant	3.00† (1.58)	8.76* (3.52)	4.10*** (.38)	4.17*** (.45)
F- statistic	1.62	2.46	9.94***	5.30**
R^2	0.09	0.13	0.47	0.33

Note. $N = 37$. All mediation tests were done using 5,000 bootstrap samples.
* $p < .05$ ** $p < .01$ *** $p < .001$.

Results of PROCESS models testing indirect effects of perceived organizational security efficacy on perceived organizational performance through communication network size and centrality are presented in Table 5. Models 1 and 2 present the effects of the organization size and perceived security efficacy on the two mediating variables, communication network size and centrality. In the presence of the control variable, the positive relationship between perceived security efficacy and communication network centrality is attenuated, but still marginally significant. Models 3 and 4 present the effects of the independent and mediator variables on the outcome, perceived performance. Both network measures are positively and significantly related to perceived performance. Indirect effects are reported using confidence intervals under Models 3 and 4. Mediation is indicated when the confidence intervals do not include zero, thus neither network size nor network performance demonstrate evidence of mediating the relationship between perceived efficacy and perceived performance, providing no support for Hypotheses 4a or 5a. In summary, results support Hypothesis 1, perceived security efficacy

is positively related to communication network centrality; Hypotheses 2 and 3 are supported, communication network size and centrality are positively and significantly related to both perceived performance and perceived benefits; and there is no evidence in support of mediation (Hypotheses 4 and 5). These results demonstrate that communication network size and centrality are independent predictors of the two outcomes, rather than mediators between the outcomes and perceived security efficacy. Additionally, these results demonstrate that perceived organizational security efficacy was positively related to performance, which was not hypothesized, but it was not associated with perceived benefit of the exercise. One possible explanation is that participants who already had strong confidence in their organization's security capability viewed the exercise as less beneficial, since they perceived limited new value to be gained. This contrasts with the consistent positive effects of communication network variables, which appear to shape both performance perceptions and perceived benefit.

5. DISCUSSION

This study contributes to the research on the effective implementation of TTX by examining the effects of factors drawn from social cognitive theory and social network theory on TTX outcomes. Few studies have examined how the "human element" affects TTX outcomes or focused on collecting data to evaluate the effectiveness of TTX implementation; thus, this research moves beyond the typical linear format to better explicate what combination of factors enhance performance and benefits in a TTX exercise, providing a more comprehensive understanding of how to implement and evaluate TTXs going forward.

Theoretical and practical implications

First, it is important to point out that the participants in general were highly engaged and perceived great benefits from the TTX exercise (mean = 6.14/7). This indicates they generally saw value, which is a necessary condition for tabletop exercises to be successful (Pearlson et al., 2021). That said**,** this research also found that employees of larger organizations with more cybersecurity professionals evaluated their organization's performance and the benefit of the exercise less favorably. One way to read this is that once a cybersecurity program is fairly mature, a standard tabletop just doesn't feel as fresh—or as revealing. If you already have solid playbooks and experienced people, the exercise may not surface many surprises, so it feels like you got less out of it. Put differently, organizations with more advanced protocols are harder to "move" with a conventional TTX, which suggests the format may need to be dialed up—more realistic scenarios, higher complexity, and sharper evaluation—so it delivers the same level of value.

Another possibility is simply that bigger, more security-mature organizations have a higher bar. When you've run a lot of exercises, dealt with real incidents, and have formal metrics, it's easier to spot what felt unrealistic, what didn't stress the right parts of the system, or what the exercise didn't actually reveal. So even if they performed "fine," participants may rate both performance and value lower because, relative to what they're used to, the TTX didn't teach them much or surface anything new.

It might be useful for practitioners to consider creating different exercises for different cohorts based on the level of cybersecurity maturity, although it is likely that participants from smaller organizations likely benefited greatly from their interactions with the participants from larger organizations (Chowdhury & Gkioulos, 2023; Mareš et al., 2024). Further research could seek to tease apart the overlapping benefits for different groups

Second, this research found that perceived security efficacy, a key social cognitive factor, is significantly associated with participants' perceptions of their organization's performance during the exercise but is not associated with their perceived benefit of the exercise. Perhaps higher confidence in their organization's security efficacy contributed to participants' effectiveness during the exercise, although an alternative explanation could be that their confidence painted a rosy picture of their performance and may have contributed to less critical attention to certain aspects of the event. Future research could augment the collection of participants' perceptions of performance with objective performance measures to compare the two. It is also interesting that enhanced confidence led participants to negatively evaluate the benefits their organizations could gain from the exercise (although the relationship was not statistically significant). Participants who view their organization as already competent often see limited value in current TTXs. This supports the first findings about perceived benefits and corroborates the suggestion that more advanced exercises may be preferable. Grouping organizations by cybersecurity maturity and security self-efficacy could also be effective.

Third, this study found that both network variables, as independent predictors, had larger effect sizes than perceived security efficacy in predicting the outcome variables, suggesting that in-exercise communication, and the access to information and influence that it provides, is an important factor to be examined further. This study also found that communication network size was a stronger predictor of both outcomes than communication network centrality, suggesting that the simpler measure might be an effective factor to consider, greatly simplifying data collection and analysis for practitioners who want to take social networks into account. Facilitators need to actively engage organizations to involve their entire network within the TTX (and probably a real cyber response) for the best outcomes.

Finally, this research learned that social cognitive and social network factors were independently related to perceived performance, with no support indicating the mediation relationship hypothesized. Neither network variable mediated the relationship between security efficacy and perceived organizational performance or perceived benefit of the exercise, although the confidence interval of the indirect effect on perceived performance through network centrality approached significance, and might have been significant with a larger sample size. Future research could dig deeper to examine other psychological readiness constructs as potential antecedents to in-exercise interaction and cooperation, which would help researchers and practitioners better prepare participants for TTXs, perhaps leading to enhanced outcomes.

Limitations and future research

Given the small sample, these findings should be interpreted cautiously. A clear next step is replication in additional settings, particularly because TTX design, facilitation, and evaluation practices vary substantially across industries and geographic regions. Future studies could also strengthen construct validity by triangulating participant perceptions with more objective indicators of exercise performance (e.g., decision timeliness and quality, coordination breakdowns, adherence to protocols, and completion of after-action items). Doing so would help assess whether perceptual biases—such as overconfidence or differences in internal performance standards—systematically shape how participants evaluate exercises. Moreover, with only 39 matched responses, the statistical power to detect mediation effects is limited. The null findings for Hypotheses 4 and 5 should therefore be interpreted with caution; the absence of statistically significant indirect effects does not necessarily indicate the absence of mediation in the population. The modest sample size elevates the risk of Type II error, particularly for the bootstrapped mediation tests, and replication with larger samples is needed before drawing definitive conclusions about the role of network position as a mechanism linking self-efficacy to TTX outcomes. At the same time, the modest sample reflects the reality of studying a live, multi-organization critical-infrastructure exercise, a setting that is difficult to access and rarely captured with matched pre– and post– and network data. In that sense, this study serves as an exploratory field-based foundation for future multi-site and longitudinal research.

Second, this study relies exclusively on self-reported perceptions of performance and benefit and cannot establish whether more favorable evaluations translate into measurable improvements in preparedness. Higher perceived gains may reflect confidence, satisfaction, or organizational norms rather than actual incident response capability. All claims about preparedness in this paper should therefore be understood as pertaining to perceived preparedness. Future work should link participant perceptions to behavioral or objective performance indicators, such as response speed, decision quality under pressure, and coordination effectiveness, to determine when perceived benefit reliably proxies actual capability.

Third, because this study is situated in a single TTX focused on electrical infrastructure within a rural Rocky Mountain West state, the findings may not generalize directly to other sectors, geographic regions, or exercise formats. The interagency coordination norms, pre-existing relationships among participants, and resource constraints characteristic of rural critical infrastructure settings may have shaped both the network structures observed and their relationship to perceived outcomes. TTXs conducted in urban settings, in different critical infrastructure sectors, or using different scenario designs and facilitation approaches may yield different patterns. These findings should therefore be treated as context-specific pending replication across diverse TTX implementations.

Fourth, the use of "especially effective communication" to define the in-exercise communication network potentially conflates effective communication with competence in cybersecurity, since individuals might perceive competence in cybersecurity as a signal of effective communication. Ultimately, reputational competence in both communication and cybersecurity expertise could reasonably affect

participants' perceptions of organizational performance and the benefits of the exercise in similar ways, but future research could use a more precise definition of effective communication to avoid any confusion on the part of participants.

Finally, although the pre–post design supports reasonable inferences about directionality, longitudinal work would provide a stronger test of how these relationships unfold over time. For example, researchers could follow the same organizations across multiple exercises (and, where feasible, real incidents) to examine whether prior TTX participation alters communication patterns, improves subsequent exercise performance, and ultimately translates into measurable preparedness gains. Such designs would also help clarify whether and how TTXs need to be adapted for more mature cybersecurity programs, where conventional formats may generate smaller marginal benefits.

6. CONCLUSION

This study had an opportunity to study a multi-organization TTX that included state and national agencies. The goal of this research was to provide novel insights into how social cognition and network factors influence the outcomes of a TTX. This study contributes to the emerging literature in TTX as these findings underscore the significant role of communication networks, specifically network size and centrality. This research also highlights the importance of security self-efficacy for performance outcomes. Practically, these results recommend structuring TTX for cohorts that may have differing maturity levels and facilitating broad and inclusive communication. The TTX exercise was designed to simulate a critical infrastructure incident to help participating organizations to be more aware of what they should do if an actual cybersecurity incident occurs.

7. REFERENCES

Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. SECURITY AND PRIVACY, 3(6), e126. https://doi.org/10.1002/spy2.126

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84(2), 191.

Bandura, A. (1997). Self-efficacy: The exercise of control. Macmillan. https://books.google.com/books?hl=en&lr=&id=eJ-PN9g_o-EC&oi=fnd&pg=PA116&dq=Bandura,+A.+(1997).+Self-Efficacy:+The+Exercise+of+Control.&ots=zAKQJZl91k&sig=G7Ptkv_fG-if4lLQORFi2kIhlQI

Bartnes, M., & Moe, N. B. (2017). Challenges in IT security preparedness exercises: A case study. Computers & Security, 67, 280–290. https://doi.org/10.1016/j.cose.2016.11.017

Borgatti, S. P., Agneessens, F., Johnson, J. C., & Everett, M. G. (2024). Analyzing social networks. https://www.torrossa.com/gs/resourceProxy?an=5730558&publisher=FZ7200

Borgatti, S. P., Everett, M. G., & Freeman, L. C. (2002). Ucinet 6 for Windows: Software for social network analysis. ResearchGate. https://www.researchgate.net/publication/216636663_UCINET_for_Windows_Software_for_social_network_analysis

Borgatti, S. P., & Li, X. (2009). On social network analysis in a supply chain context. Journal of Supply Chain Management, 45(2), 5–23.

Borgatti, S. P., Mehra, A., Brass, D. J., & Labianca, G. (2009). Network Analysis in the Social Sciences. Science, 323(5916), 892–895. https://doi.org/10.1126/science.1165821

Brass, D. J. (1984). Being in the Right Place: A Structural Analysis of Individual Influence in an Organization. Administrative Science Quarterly, 29(4), 518. https://doi.org/10.2307/2392937

Brilingaitė, A., Bukauskas, L., Juozapavičius, A., & Kutka, E. (2022). Overcoming information-sharing challenges in cyber defence exercises. Journal of Cybersecurity, 8(1), tyac001. https://doi.org/10.1093/cybsec/tyac001

Brunner, J., & Lewis, D. (2006, December). Tabletop Exercises Can Train All the Staff for Safety. The Education Digest, 72(4), 46–49.

Burt, R. S. (1992). Structural Holes: The Social Structure of Competition (SSRN Scholarly Paper No. 1496205). Social Science Research Network. https://papers.ssrn.com/abstract=1496205

Cammann, C., Fichman, M., Jenkins, D., & Klesh, J. (1979). The Michigan organizational Assessment Questionnaire. Unpublished Manuscript, University of Michigan, Ann Arbor, 10.

Carley, K. M. (n.d.). DYNAMIC NETWORK ANALYSIS.

Carley, K. M. (2020). Social cybersecurity: An emerging science. Computational and Mathematical Organization Theory, 26(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9

Chowdhury, N., & Gkioulos, V. (2023). A Framework for Developing Tabletop Cybersecurity Exercises. In S. Katsikas, F. Cuppens, C. Kalloniatis, J. Mylopoulos, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, M. A. Sotelo Monge, M. Albanese, B. Katt, S. Pirbhulal, & A. Shukla (Eds.), Computer Security. ESORICS 2022 International Workshops (Vol. 13785, pp. 116–133). Springer International Publishing. https://doi.org/10.1007/978-3-031-25460-4_7

Compeau, D., Correia, J., & Thatcher, J. (2022). When Constructs Become Obsolete: A Systematic Approach to Evaluating and Updating Constructs for Information Systems Research. Management Information Systems Quarterly, 46(2), 679–712.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. MIS Quarterly, 19(2), 189.

Cybersecurity & Infrastructure Security Agency. (2025). CISA Tabletop Exercise Packages | CISA. https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

Durcikova, A., Miranda, S. M., Jensen, M. L., & Wright, R. T. (2024). United We Stand, Divided We Fall: An Autogenic Perspective on Empowering Cybersecurity in Organizations. MIS Quarterly, 48(4), 1503–1536. https://doi.org/10.25300/misq/2024/17211

Elvegård, R., & Andreassen, N. (2024). Exercise design for interagency collaboration training: The case of maritime nuclear emergency management tabletop exercises. Journal of Contingencies and Crisis Management, 32(1), e12517. https://doi.org/10.1111/1468-5973.12517

Evans, C. A. (2019). Tabletop exercises in the nursing classroom: An introduction for nurse educators. Nursing Forum, 54(4), 669–674. https://doi.org/10.1111/nuf.12394

Everbridge. (2025, April 9). What is a Tabletop Exercise? Everbridge. https://www.everbridge.com/blog/conducting-effective-tabletop-exercises-for-emergency-preparedness/

Freeman, L. C. (1978). Centrality in social networks conceptual clarification. Social Networks, 1(3), 215–239. https://doi.org/10.1016/0378-8733(78)90021-7

Freeman, L. C., Romney, A. K., & Freeman, S. C. (1987). Cognitive Structure and Informant Accuracy. American Anthropologist, 89(2), 310–325. https://doi.org/10.1525/aa.1987.89.2.02a00020

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy, 22(6), 461–485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., & Good, T. (2006). Guide to test, training, and exercise programs for IT plans and capabilities. NIST. https://www.nist.gov/publications/guide-test-training-and-exercise-programs-it-plans-and-capabilities

Gross, M., & Ho, S. M. (2021). Collective Learning for Developing Cyber Defense Consciousness: An Activity System Analysis. 32.

Haddouch, R., Clouse, S. F., Wright, R. T., Floyd, T., & Akello, P. (2025). Strengthening Incident Response: Lessons from Cybersecurity Tabletop Exercises for Rural Critical Infrastructure. Cybersecurity Pedagogy & Practice Journal, 4(2), 4–35. https://doi.org/https://doi.org/10.62273/SACF5628

Hayes, A. F. (2012). PROCESS: A versatile computational tool for observed variable mediation, moderation, and conditional process modeling. University of Kansas, KS. https://www.researchgate.net/profile/Ludmila-Zajac-Lamparska/post/How-can-I-analyze-baseline-measures-as-predictors-of-change-in-longitudinal-designs/attachment/59d61de779197b807797c2a0/AS%3A273843497701387%401442300786437/download/Hayes+process.pdf

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior

and the protection motivation theory. Computers & Security, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, 34(3), 549–566. https://doi.org/10.2307/25750691

Judge, T. A., & Bono, J. E. (2001). Relationship of core self-evaluations traits—self-esteem, generalized self-efficacy, locus of control, and emotional stability—with job satisfaction and job performance: A meta-analysis. Journal of Applied Psychology, 86(1), 80–92. https://doi.org/10.1037/0021-9010.86.1.80

Leyden, J. (2025, June 17). Operation 999: Ransomware tabletop tests cyber execs' response | CSO Online. https://www.csoonline.com/article/4006349/operation-999-ransomware-tabletop-tests-cyber-execs-response.html

Ling, J. (2025, June 2). The US Grid Attack Looming on the Horizon. Wired. https://www.wired.com/story/youre-not-ready-for-a-grid-attack/

Maennel, K., Brilingaitė, A., Bukauskas, L., Juozapavičius, A., Knox, B. J., Lugo, R. G., Maennel, O., Majore, G., & Sütterlin, S. (2023). A Multidimensional Cyber Defense Exercise: Emphasis on Emotional, Social, and Cognitive Aspects. SAGE Open, 13(1), 21582440231156367. https://doi.org/10.1177/21582440231156367

Mareš, M., Chytilek, R., Špačková, Z., Drmola, J., Hrbková, L., Mlejnková, P., & Tóth, M. (2024). Assessment of performance during cybersecurity tabletop exercises. Security Journal, 37(3), 712–735. https://doi.org/10.1057/s41284-023-00391-4

Maurer, T. (2023, September 18). 6 Actions CEOs Must Take During a Cyberattack. Harvard Business Review. https://hbr.org/2023/09/6-actions-ceos-must-take-during-a-cyberattack

Mirzaei, S., Eftekhari, A., Sadeghian, M. R., Kazemi, S., & Nadjarzadeh, A. (2020). The Effect of Disaster Management Training Program on Knowledge, Attitude, and Practice of Hospital Staffs in Natural Disasters. Journal of Disaster and Emergency Research, 2(1), 9–16.

Monge, P. R., & Contractor, N. (2003). Theories of Communication Networks. Oxford University Press. https://doi.org/10.1093/oso/9780195160369.001.0001

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

NUARI: Addressing National Cyber Security Issues. (n.d.). Retrieved September 7, 2024, from https://nuari.org

Park, H., & Shin, S. (2022). When Does Group Efficacy Deteriorate Group Performance? Implications of Group Competency. Behavioral Sciences, 12(10), 379. https://doi.org/10.3390/bs12100379

Pate, A., Bratberg, J. P., Robertson, C., & Smith, G. (2016). Evaluation of a Tabletop Emergency Preparedness Exercise for Pharmacy Students. American Journal of Pharmaceutical Education, 80(3), 50. https://doi.org/10.5688/ajpe80350

Pearlson, K., Thorson, B., Madnick, S., & Coden, M. (2021). Cyberattacks are inevitable. Is your company prepared. Cybersecurity And Digital Privacy, Harvard Business Review. https://cams.mit.edu/wp-content/uploads/2021-03-09-v3-LIVE-HBR-Cyberattacks-Are-Inevitable.-Is-Your-Company-Prepared1.pdf

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. Behavior Research Methods, 40(3), 879–891. https://doi.org/10.3758/BRM.40.3.879

Radow, L. J. (2007). Tabletop exercise guidelines for planned events and unplanned incidents/emergencies. https://trid.trb.org/View/1152626

Staples, D. S., Hulland, J. S., & Higgins, C. A. (1999). A Self-Efficacy Theory Explanation for the Management of Remote Workers in Virtual Organizations. Organization Science, 10(6), 758–776. https://doi.org/10.1287/orsc.10.6.758

Stavrou, E., & Piki, A. (2024). Cultivating self-efficacy to empower professionals' re-up skilling in cybersecurity. Information & Computer Security, 32(4), 523–541.

Tasselli, S., Kilduff, M., & Menges, J. I. (2015). The Microfoundations of Organizational Social

Networks: A Review and an Agenda for Future Research. Journal of Management, 41(5), 1361–1387. https://doi.org/10.1177/0149206315573996

Ter Huurne, E. F. J., & Gutteling, J. M. (2009). How to trust? The importance of self-efficacy and social trust in public responses to industrial risks. Journal of Risk Research, 12(6), 809–824. https://doi.org/10.1080/13669870902726091

Tobergte, P., Landsberg, L., & Knispel, A. (2022). Evaluation of Tabletop Exercises in Emergency Response Research and Application in the Research Project SORTIE.

Valente, T. W., & Foreman, R. K. (1998). Integration and radiality: Measuring the extent of an individual's connectedness and reachability in a network. Social Networks, 20(1), 89–105. https://doi.org/10.1016/S0378-8733(97)00007-5

Vykopal, J., Čeleda, P., Švábenský, V., Hofbauer, M., & Horák, M. (2024). Research and Practice of Delivering Tabletop Exercises. Proceedings of the 2024 on Innovation and Technology in Computer Science Education V. 1, 220–226. https://doi.org/10.1145/3649217.3653642

White, G. B., Dietrich, G., & Goles, T. (2004). Cyber security exercises: Testing an organization's ability to prevent, detect, and respond to cyber security events. 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of The, 10 pp. https://doi.org/10.1109/HICSS.2004.1265411

Wolf, E. J., Harrington, K. M., Clark, S. L., & Miller, M. W. (2013). Sample Size Requirements for Structural Equation Models: An Evaluation of Power, Bias, and Solution Propriety. Educational and Psychological Measurement, 73(6), 913–934. https://doi.org/10.1177/0013164413495237

Wright, R. T., Johnson, S. L., & Kitchens, B. (2023). Phishing Susceptibility in Context: A Multilevel Information Processing Perspective on Deception Detection. MIS Quarterly, 47(2).

Wu, J.-H., & Wang, Y.-M. (2006). Measuring KMS success: A respecification of the DeLone and McLean's model. Information & Management, 43(6), 728–739. https://doi.org/10.1016/j.im.2006.05.002

Young, J., & Farshadkhah, S. (2022). Teaching Cybersecurity Incident Response Using the Backdoors & Breaches Tabletop Exercise Game. Cybersecurity Pedagogy & Practice Journal. http://www.cppj.info/2022-1/n1/CPPJv1n1.pdf#page=4

Appendix

Appendix 1. TTX Exercise.

Electrical Grid TTX1 Modules and Questions

Event Purpose: The United States will continue to face critical risk to its critical infrastructure from state, non-state actors and criminal networks. The state as a rural state continues to be at risk from limited resources and critical national investment in protecting critical infrastructure. As part of the nation's critical infrastructure, 3 sectors stand out as critical to national functions: electricity, telecommunications, and finance. Known as the tri-sector; they hold most of the critical national functions critical to state functions. This exercise is designed to be the start of a series of cyber incident response exercises to discover gaps, vulnerabilities and most importantly solutions to cross sector and cross function incident response. The integration of government, industry, military, and academia provides a strategic opportunity to work toward informed state-wide solutions with a robust network of partners.
Participants: Public Energy Utility (electrical generation, transmission, and distribution), twenty electric distribution cooperatives, National Guard, State fusion center, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), and a state university.
Scenario: Tensions continue to rise in globally as China threatens Taiwan for strong returns in their most recent Presidential election for a candidate that emphasized a free and independent Taiwan and elimination of the one China policy. China in turn has ramped up mobilization of PLA and PLN resources forecasting a lethal response or invasion to repulse an independent Taiwan recognized by global powers. China has also ramped up greater cyber intrusions on US national infrastructure, interested in strategic US military facilities for force projection, nuclear response, and mobilization. These intrusions are focused on US military systems, defense industrial base systems and critical components of the electric grid supporting military installations and outlying Strategic Command facilities.
Exercise Objectives:

- Identify key relationships in an escalatory cyber incident in an electric distribution scenario.
- Identify key organizational capability gaps in responding to an escalatory cyber incident (local/State/federal)
  - Training and education gaps
  - Authorities and policy gaps
  - Response capabilities and capacity
  - Process and relationships
- Identify the key processes for cross organizational escalatory cyber incident
- Identify key questions and decisions required at private-public interface (local/state)
- Identify what resources are available from the federal government (specific organizations) to enhance state, local government, and industry

Training Objectives for Organizations

Industry Partners:

- Identify key decisions and processes required in an escalatory cyber incident
- Develop relationships and mature processes to respond to an escalatory cyber incident
- Develop basic gaps analysis for organizational response plan
- Identification of war stoppers, policy and authority issues with partner (local/state/federal)
- Identify resource requirements to enhance incident response planning and exercising
- Identify outside resources available and the process for requesting support during a cyber incident

State Government

- Identify key decisions and processes required in an escalatory cyber incident

- Develop relationships and mature processes to respond to an escalatory cyber incident
- Develop basic gaps analysis for state response plan
- Identification of war stoppers, policy and authority issues with partner (local/state/federal)
- Identify resource requirements to enhance incident response planning and exercising
- Identify outside (Federal) resources available and process to request for cyber incident

National Guard

- Identify and describe National Guard capabilities available to the state for cyber event
- Identify authorities, policy gaps to respond to state cyber incident and interaction with private industry (what can they do and what are they capable of doing)
- Identify reporting requirements and the approval process for cyber incident response (e.g., the 9-line program)
- Identify capability and capacity gaps for state response to cyber incident response

University

- Identify opportunities to support gaps analysis and requirements development
- Identify opportunities for university leadership
- Identify opportunities for workforce professional development (future workforce and professional development of current workforce)

Deliverables:

- Student-Observer, Researcher and DECIDE questions data
- After action report on key objectives above
- Researcher whitepaper on Identified gaps from exercise
- Proposals (Roadmap) for series of exercises (annual/semi-annual or quarterly)
- Gaps analysis report (internal with partners)

Tabletop Scenario

Module 1

Day 1 – Wednesday April 19th

Your industrial control system (ICS) software provider recommends a new critical security update for its industrial control systems in the upcoming weeks. The patch is downloaded by a staff engineer's laptop and then uploaded to your system's Programmable Logic Controller(s) (PLC).

Discussion Questions

1. What is the greatest cyber threat to your organization? To the energy sector?
2. What processes are in place to vet third-party vendors and their patches (software authenticity & integrity checks)
3. Describe the security controls in place for the engineer's laptop.
4. How are personnel who update ICS systems vetted and trained?

Day 2 – Thursday April 20th

The Cybersecurity Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) released a joint alert regarding a phishing campaign targeting energy companies over the past three months. A suspected global hacker group has been observed discussing on dark web forums a sophisticated phishing strategy to cast a wide net to attack as many energy sector businesses and ICS systems as possible.

Your organization also receives information from other cyber intelligence sources that report incidents of threatening notes and emails being delivered, information on a widespread phishing campaign against a bank, and known malicious actor groups.

Day 6 – Monday April 24th

All Electricity Information Sharing and Analysis Center (E-ISAC) members receive an email alert from "alerts@Energy-ISAC.co". The alert warns members regarding threats to the electrical grid via a watering hole on websites frequented by organization employees. The alert is quickly identified as a spoof by E-ISAC, and you are notified via E-ISAC Portal Notification "noreply@mail.eisac.com" of its untrustworthiness. CISA and FBI amplify E-ISAC's Portal Notification for situational awareness.

Discussion Questions

1. What actions would you take based on the alerts in this scenario?
2. What cybersecurity threat intelligence do you currently receive?
   a. What cybersecurity threat intelligence is most useful?
   b. How is the information shared internally?
   c. How do you assess intelligence to determine its relevance?
   d. When you receive a significant number of alerts/reports from many different sources, what process is used to identify the most important/actionable information?
3. With different types of intelligence (physical vs cyber, electric sector vs general cyber activity, local vs national/global), how does your organization balance these different intelligence topics/sources?
4. What factors are considered for you to determine an intelligence source to be trustworthy?
5. Given the false information received in the above incident, what factors would you consider for attempting to validate any other intelligence you receive?
   a. What internal/external partners would you contact to validate these sources?
   b. How would you contact trustworthy intelligence sources?
6. What alternative methods can intelligence be shared if normal channels are compromised or potentially untrustworthy?

Day 7 – Tuesday April 25th

A spear-phishing email is received by your operators of the transmission system from a typo-squatting energy provider account. The email asks the target to change their credentials that access the Market Portal. Some in your organization report the email to their management or security officer; others complete the request to change passwords/credentials.

Discussion Questions

1. Describe your organization's cybersecurity awareness training program.
2. What topics does the training address?
   a. How often are personnel required to complete the training?
   b. Are simulated phishing emails included in the training?
   c. What are the consequences for not completing training?
   d. How do you track and enforce cybersecurity awareness training?
3. How do employees report possible phishing emails?
   a. What actions are taken after a phishing email is reported?
4. How/What is the process in place you would use to share this intel with other organizations?
5. Because it appears as though the energy provider has been potentially compromised, how would you handle validating the energy provider's communications?
6. What communication/expectation would you have from the energy provider in addressing this issue?
7. What alternative communications/reporting methods are available?

Module 2

Day 8 – Wednesday April 26th

Breakers begin opening and closing on electric equipment on the grid. The alternating breakers are becoming erratic enough to cause intermittent outages. An investigation is opened to discover the root cause of the breaker issues.

Discussion Questions:

1. At what point would you notify law enforcement, regulators, or others in government of these incidents?
   a. What are the thresholds for requesting external assistance?
2. What resources would you need to manage these incidents?
   a. What resources are immediately available?
   b. What outside partners, if any, would you contact for assistance or advice?
3. How are you communicating with your operations teams that are trying to stabilize the grid?

Day 10 – Friday April 28th

Residents and business owners begin calling customer service and your operations center regarding the outages. Some customers report that the intermittent power issue is tripping their emergency generators.

Day 13 – Monday May 1st

Throughout the night, affected residents take to social media sites, including your company's online platforms, to complain about the lack of power, claiming their calls to the operations center and customer service are being ignored.

As workers continue to troubleshoot around the clock, for every load reenergized, another indicator alerts to a power loss. More customers call in to report outages.

Your customer service and your operations center receive calls from local healthcare providers regarding continued outages and letting the operations center know of failures in their local backup generator.

Discussion Questions

1. Who is authorized to represent the company on social media? To the news network media?
2. How would you manage interactions with the media or the public?
3. What are employees supposed to do if they are contacted by media?
4. How do you share information internally?
5. Do you provide media training to team members to react to these incidents?
6. As these events play out, who do you share information with?
    a. What information do you share? Who does the sharing?
    b. How do the Electrical Coop Association members support each other?
    c. How does the Electrical Coop Association and the public utility support each other?
7. Could any of the events described in this module be classified as cybersecurity incidents? If so, how should they be handled?
8. At what point would you refer to your cybersecurity incident response plan?
    a. How would you handle this incident per the plan?
    b. How are your cyber/physical plans coordinated during incident response?

Day 15 – Wednesday May 3rd

Local police receive multiple reports of individuals taking photographs of transmission lines, transformers, and electric substations. Although no suspects were questioned to date, some reports indicate that the individual may have been dressed in a uniform resembling those local utility workers wear and may have had a backpack containing tools. Concurrently, other electric cooperatives observed some suspicious activity at a few of its electric substations.

Recently, the Federal Bureau of Investigation (FBI) released a Joint Intelligence Bulletin (JIB) warning of possible sabotage to telephone lines, specifically those relating to 911 services. In response to the JIB, the Electricity Information Sharing and Analysis Center (E-ISAC) issued an industry advisory concerning the need for increased vigilance and reporting of suspicious activity.

Discussion Questions

1. Has state Electric Cooperative Association members and the public power company identified to law enforcement the level of importance of regional and local critical infrastructure (e.g., electric substation, communications, and electrical vaults)?
2. What security or intruder detection measures are employed at both above ground and underground communication vaults? At local electric substations?
3. If your organization received information related to "suspicious behavior" or potential threats against your facilities and personnel, how would you communicate this information to appropriate industry partners or authorities?
    a. What are your local reporting procedures (e.g., local suspicious activity reporting [SAR]), and which entities would you notify?
    b. Is your organization aware of the Nationwide SAR Initiative?
    c. Is your organization familiar with how to contact your local law enforcement, Joint Terrorism Task Force (JTTF), state fusion center, FBI Office, and local CISA Protective Security Advisor (PSA)?

4. What measures might you ask of local law enforcement at this time to protect your organization and / or facilities (e.g., outreach, increased vigilance)?
5. What internal information sharing and dissemination processes does your organization currently use?
    a. How does your organization triage the information it receives (e.g., formal reporting, rumors, social media) for further dissemination within the organization and to personnel?
    b. Are nationwide trends of suspicious behaviors within your industry and across the Energy Sector tracked locally?
    c. Who is responsible for coordinating the risk communications message for your organization?
    d. How would implementation of protective measures be communicated?
    e. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing or prohibit use of electronic communication during specific times?
6. Given current and established information sharing procedures, what types of official information are the most useful (immediate information versus analyzed information) to your organization?
    a. Does your organization use the Homeland Security Information Network – Critical Infrastructure – Electricity (HSIN-CI - Electricity) portal?
    b. Does your office habitually receive E-ISAC Industry Advisories or JIBs that are pertinent to your organization?
    c. Does your organization receive security threats or protective measure information from trade organizations, manufacturers, consultants, or other industry partners?
    d. Does your organization perform independent analysis on information provided? If so, describe the process?

Module 3

Day 20 – Monday May 8th

Grid Operations Center crews notice the turbine over rev is exceeding recommended operational revolutions per minute. Two issues develop: electrical output is increased beyond the level transformers can handle, and the turbine starts to fail from the heat generated along its power shaft. As the turbine spins out of control, crews attempt to conduct an emergency shutdown. However, they are unable to completely de-energize the system before the transformers fail. This creates a cascading effect across the grid as it attempts to keep up the demand for electricity.

Day 21 – Tuesday May 9th

As state energy companies attempt to recover from the cyber incident, it is discovered that replacement turbine parts are delayed 6-12 months due to supply chain issues.

Discussion Questions

1. How do you manage crews (Field or Operation Center Crews) across days of repairing energy grids?
2. How are systems/grids prioritized for recovery efforts?
    a. How do you determine the criticality of each system/grid?
    b. How is this defined by your business continuity and recovery plans?
    c. What backup systems can be deployed?
        i. How quickly can they be deployed?
        ii. How are they verified and updated?
3. How do you share resources among other electric sector members in the event of a major grid issue?
4. How are field crews communicating back to respective Controls Rooms to provide updates/assessments on the state of grid equipment?
5. How do grid failures impact the stability/energy flows across the greater state Interconnection?
    a. What type of communication is happening with other regions in the state?
6. How does this impact the running of other parts of the business (such as the Markets)?
7. What information would you share with the media?
8. How does the delays in replacement parts impact grid recovery and reliability?
9. Given the new timeline on repairing equipment (6-12 months out) how does this impact the running of other parts of the business (such as the Markets)

Day 22 – Wednesday May 10th

After a thorough investigation, it was discovered that the malfunctioning grid and transformers were a result of a patch containing malware that infected industrial control systems (ICS).

Day 23 – Thursday May 11th

Several media outlets contact your organization seeking comments about the increasing power outages. Local new stations around the state report of healthcare providers, small businesses, schools, and government facilities are struggling with providing services due to the increasing power outages. The report states that businesses that have backup generation have not properly tested their backup equipment and they are not working properly.

Discussion Questions

1. What is your change management process to determine if any other update/upgrade could also be contributing?
2. How do you determine if a recent software patch has adversely affected your systems?
3. What processes and resources are in place for cyber evidence preservation and forensics?
    a. At this point what information are you sharing with external partners (particularly those participating in this exercise)
4. How are you balancing decisions around executing your cybersecurity incident response plans to contain & eradicate while also keeping the grid running?
5. What level of risk are you willing to accept to keep the electric grid running when you have software/equipment that has been compromised?
6. If you find that other organizations are also victims of these incidents, what factors are considered for sharing incident information? What value is there in sharing? What channels/capabilities do you have for open sharing incident information?
7. What outside partners, if any, would you contact for assistance or advice
8. For the State and Federal partners in the room, at this point how can you be of assistance?
9. How do you determine if an attacker is in or still in your system?
10. How do you monitor suspicious or anomalous network activity for IT systems?
11. How do you recover your Industrial Control Systems?
12. IT Backups vs OT Backups. Are they the same? Where are the backups stored? Are they offline or online, stored in a secure location, or managed by a third party?
    a. Are backups tested to ensure they work and are not corrupted, infected, or damaged?
    b. How far back can your backups recover?
    c. How often is the data restoration process exercised?
13. What information would you share with the media?
    a. Would you share any information about the malware with the media?

Module 4

Day 25 – Saturday May 13th

Residents experience disruptions in attempts to place and receive 911 calls using their landline telephones. Citizens that were unable to place landline calls successfully used mobile telecommunications to notify 911 operators and their telephone service providers of the problem.

The location of the communications disruption is determined to be near an electric substation. Local Co-op workers are dispatched to the site and begin surveying to determine the locality and cause of the disruption.

Law enforcement officers are dispatched to a local electric substation after receiving reports of sporadic gunfire being directed at the substation. Meanwhile, the local electric utility company facility operators notice system abnormalities and begin implementing safety protocols. After a cursory search around the perimeter of the substation facility, police officers discover several "large metal boxes" leaking fluid, possibly oil.

Upon analysis, state's Analysis and Technical Information Center which is the state's Fusion Center determines that this closely resembles an event outlined in an E-ISAC Portal Notification from Day 15 – May 3rd. When this information is forwarded to the local FBI Field Office, they issue a JIB for release to local law enforcement and the private sector, stating that this is a recurring method of sabotage.

Discussion Questions

1. Would the electric utility company be notified by the telecommunications company of the communications disruption or vice versa of any power disruption?
   a. Would the 911 dispatch office contact either the electric company or telecommunication company to report any disruption of service or inquire about the duration for repair?
   b. Should there be more sharing of real-time information between telecommunication and electric substation entities, particularly when interruption of communications may be an initial sign of an attack?
2. Are first responders (e.g., law enforcement, fire fighters, and emergency services) aware of any specific concerns or hazards associated with responding to incidents at electric substations?
3. Do your organization's emergency response plans (e.g., site security plans, emergency evacuation plans, emergency action plans, or other appropriate plans) contain protocol for properly responding to incidents described in this module?
   a. How often does your organization review its emergency response plans, and does it perform drills to test their effectiveness?
   b. Do your organization's response plans address how to coordinate power restoration priorities?
   c. Do your organization's response plans account for law enforcement evidence-gathering requirements?
   d. Have cross-sector dependencies been incorporated into your organization's response plans?
   e. Have resulting impacts or cascading effects on other electricity components within the Energy Sector been incorporated into your organization's response plans?
4. What information sharing processes would you use to disseminate information concerning this incident?
   a. What notification capabilities would you use to share information and communicate protective measures implementation?
   b. How would employee safety concerns be managed (e.g., at what point would the utility company allow employees to enter the site)?
   c. What are your organization's external information sharing responsibilities in response to such incidents?
   d. How would proprietary information concerns be managed?
   e. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing or prohibit use of electronic communication during specific times?
5. What protective security measures would be employed following a domestic attack?
   a. Would you coordinate protective measure implementation with any organization within the Electricity Subsector or specific government entities, such as law enforcement agencies and your CISA PSA?
   b. Would you need to communicate implemented protective measures to organizational liaisons, response entities??
   c. How useful are the information bulletins and advisories the U.S. Department of Homeland Security (DHS) provides (e.g., a JIB) that recommend protective measures?

Final Discussion Questions

1. When is an incident determined to be over?
2. How do you document incident lessons learned?
3. What are your after-action (post-incident) procedures?
4. How do you document and implement improvement plan processes?

Appendix 2. Scale Items and Confirmatory Factor Analysis.

Scale	Variance explained	Cronbach's Alpha	Items	Factor Loadings
Perceived organizational performance	60.2%	0.862	Our organization exceeded its objectives for dealing with this cyber incident.	0.748
			Reports on our organization's performance in dealing with cyber incidents are favorable.	0.712
			Our organization successfully dealt with this cyber incident.	0.865
			Overall, I am satisfied with the outcome we achieved through the tabletop exercise.	0.749
			Overall, we handled the problems in the tabletop exercise well.	0.802
			I am satisfied with our performance during the tabletop exercise.	0.769
Perceived benefit of the exercise	79.8%	0.865	The tabletop exercise helped my organization acquire new knowledge when dealing with cybersecurity incidents.	0.944
			The table top exercise helped my organization understand its weaknesses when dealing with cybersecurity incidents.	0.834
			The tabletop exercise will benefit my organization.	0.898
Perceived organizational security efficacy	90.4%	0.945	My organization has above-average ability in responding to cybersecurity events.	0.970
			My organization has the resources to respond appropriately to cyber incidents compared to other organizations.	0.947
			The members of my organization have excellent skills for dealing with cyber incidents.	0.935

* Confirmatory Factor Analysis with varimax rotation; N = 43. Variance explained is of the single factor identified in each analysis.

Appendix 3. Frequencies for Categorical Control Variables.

Variable		N	Valid %
In-person or virtual attendance	In person	43	93.5
	Virtual	3	6.5
Affiliation	CISA	4	8.7
	Electric Company	3	6.5
	Electric Co-op	22	47.8
	National Guard	9	19.6
	NGO	2	4.3
	State/Local Govt	6	13.0
Rank in home organization	Individual Contributor	26	57.8
	Supervisor/Manager	13	28.9
	Director	4	8.9
	VP or SVP	1	2.2
	Top Management Team	1	2.2
Position Tenure	Less than 1 year	5	12.5
	1-3 years	13	32.5
	3-7 years	8	20.0
	7-12 years	4	10.0
	More than 12 years	10	25.0
Age	25-34 years	3	7.7
	35-44 years	17	43.6
	45-54 years	11	28.2
	55-64 years	8	20.5
Gender	Female	9	23.1
	Males	28	71.8
	Non-binary	1	2.6
	Prefer not to respond	1	2.6
Race	Hispanic or Latino	3	7.7
	White	33	84.6
	Prefer not to respond	3	7.7
Veteran status	Not a veteran	36	80.0
	Veteran	6	13.3
	Prefer not to respond	3	6.7

Semantic Technologies for Cybersecurity Education Competencies: JSON-LD Implementation of Distributed Learning Analytics

Ryan Straight
ryanstraight@arizona.edu

Aaron Escamilla
escamillaa@arizona.edu

University of Arizona
Tucson, AZ 85721, USA

Abstract

Educational technologies struggle to represent the human-AI collaborative competencies increasingly central to cybersecurity practice. Current learning management systems and assessment frameworks assume individual human learners interacting with passive technological tools, failing to capture the distributed agency and technological mediation that characterize contemporary professional work. This research addresses these limitations by developing semantic web representations of posthumanist educational concepts using JSON-LD schemas. Through systematic analysis of the NICE Cybersecurity Workforce Framework, we demonstrate how qualitative posthumanist coding can be translated into machine-readable formats while preserving theoretical sophistication. Using the Technology Portfolio Management work role as a detailed case study, we show how JSON-LD enables computational analysis of human-technology entanglement patterns in professional competencies. The resulting semantic framework supports SPARQL queries that identify collaborative learning processes, technological mediation patterns, and distributed agency requirements across cybersecurity roles. This methodology provides a practical pathway for developing educational technologies that recognize learning as emerging through human-AI assemblages rather than occurring within isolated human subjects. Results demonstrate the feasibility of operationalizing posthumanist theory for educational technology design, offering new possibilities for curriculum development and assessment in domains where human-AI collaboration is fundamental to professional practice.

Keywords: Posthumanism, Semantic Web, JSON-LD, Educational Technology, Human-AI Collaboration, Learning Analytics

Recommended Citation: Straight, R., Escamilla, A., (2026). Semantic Technologies for Cybersecurity Education Competencies: JSON-LD Implementation of Distributed Learning Analytics. *Cybersecurity Pedagogy and Practice Journal;* v5(n1) pp 79-103. DOI# https://doi.org/10.62273/SCRC1853

Semantic Technologies for Cybersecurity Education Competencies: JSON-LD Implementation of Distributed Learning Analytics

Ryan Straight and Aaron Escamilla

1. INTRODUCTION

Current educational technology systems are largely built on human-centered assumptions that position learners as autonomous agents and treat AI systems as neutral instruments that simply support personal achievement (Cukurova, 2025). Learning management systems track discrete individual metrics, adaptive learning platforms modify content delivery based on presumed cognitive deficits, and learning analytics models predict outcomes while bracketing out the complex socio-technical assemblages that actually constitute contemporary learning environments. This paradigm obscures the entanglements between humans and technological systems that characterize knowledge emergence in digitally-mediated contexts.

Posthumanist and postphenomenological perspectives challenge this dominant framing by conceptualizing agency as distributed across human and non-human actors within technological assemblages (Taylor & Hughes, 2016; Rosenberger & Verbeek, 2015). Rather than treating technology as external support, posthumanism reveals how AI systems actively enact, shape, and co-constitute learning processes in ways that transform rather than merely extend human capabilities (Adams & Thompson, 2016). These mediators fundamentally reshape meaning and the ontological status as knowledge moves across contexts, challenging assumptions about stable learning objects and linear knowledge transfer (Gourlay, 2015).

Cybersecurity education offers a compelling domain for investigating these dynamic approaches, as professional practice increasingly involves human-AI collaboration. Security analysts routinely work alongside automated detection systems, threat intelligence platforms, and decision support tools in ways that blur traditional boundaries between human and machine agency. Our previous analysis of the NICE Cybersecurity Workforce Framework (V1) (Newhouse et al., 2017) education-focused work roles revealed that 89.4% of competency statements contained elements consistent with posthumanist conceptions of learning, including recurring patterns of co-adaptation between human and technological systems, suggesting that cybersecurity education already reflects an understanding of learning as fundamentally entangled and distributed across human and technical actors (Straight, 2024).

This work operationalizes these insights through posthumanist insights, namely semantic technologies, specifically the use of JavaScript Object Notation for Linked Data (JSON-LD) schemas to represent distributed agency, technological mediation, and collaborative knowledge construction in machine-readable formats. Rather than forcing posthumanist concepts into traditional human-centered data structures, we develop a vocabulary and relationship model that preserve theoretical nuance while enabling practical application. The contribution extends beyond cybersecurity education by providing methodological frameworks for representing human-AI collaboration across domains where conventional learning analytics inadequately capture the complexity of contemporary knowledge work.

Before introducing the technical implementation of this semantic framework, we first establish its theoretical foundations. The following section elaborates how posthumanist perspectives disrupt anthropocentric assumptions embedded in prevailing educational technology architectures, providing the conceptual grounding necessary for understanding why JSON-LD schemas require fundamentally different representational strategies than those employed in human-centered learning analytics systems.

2. POSTHUMANISM IN EDUCATIONAL CONTEXT

Traditional approaches to educational technology assume learning occurs within individual human minds, with technology serving as delivery mechanism or assessment tools (Shutkin, 2019). Such designs embed anthropocentric assumptions about agency, cognition, and knowledge that posthumanist theory

fundamentally challenges (Braidotti, 2019). Educational AI systems assume autonomous, rational human subjects as sole loci of agency, representing learners as independent agents whose behaviors can be predicted and optimized through data analytics (Oshiesh, 2025; Akintola et al., 2025). This individualistic model fails to account for posthumanist insights about agency as distributed across human and non-human actors—including technologies, algorithms, and environmental factors that actively participate in rather than simply support learning processes.

These platform designs employ transmission models where knowledge represents pre-defined content delivered and measured through standardized assessments, failing to account for learning as emergent and relational (Schlyter et al., 2012). Data-driven models treat assessment as neutral processes that quantify and predict performance, obscuring the performative and political dimensions that posthumanist perspectives reveal as reinforcing dominant power structures while marginalizing alternative ways of knowing.

Learning is thus revealed as emerging through dynamic interactions between human learners, educational content, technological interfaces, algorithmic processes, and institutional structures. Rather than occurring "in" individual minds, learning happens "between" and "through" these actors in ways that challenge traditional subject-object distinctions. This perspective suggests educational technologies should represent learning processes as collaborative achievements rather than individual accomplishments, fundamentally altering how we conceptualize assessment, curriculum design, and educational AI ethics.

Minimal attention is given to mediating effects of educational technologies, treating them as implementation details rather than fundamental aspects of learning processes (Bower, 2019). Assumptions that technological mediation can be separated from learning content reflect the problematic notion that texts maintain stable meanings across digital contexts, when the movement between print-based and digital media involves constant transformation of both content and significance (Gourlay, 2015).

A postphenomenological analysis demonstrates that technologies actively mediate human experience rather than serving as neutral conduits for information transfer. When students interact with educational AI systems, these technologies shape perception, attention, and understanding in ways that extend beyond simple content delivery to constitute the very conditions under which learning becomes possible. Recommendation algorithms influence what knowledge appears relevant and accessible, interface designs shape how concepts are understood and connected, and assessment systems mediate how learning is recognized, validated, and institutionally credentialized.

Recognizing technological mediation as constitutive of learning rather than merely supportive would require learning analytics that evaluate human-AI collaboration effectiveness rather than individual human performance metrics, curriculum designs that explicitly address how AI systems influence perception and decision-making rather than simply teaching tool usage, and assessment approaches that recognize collaborative competencies as legitimate educational outcomes.

Distributed Agency and Collaborative Knowledge Construction

Posthumanist theory challenges the assumption that agency resides exclusively within human actors. In contemporary learning environments, algorithmic systems make decisions about content presentation, pacing, and assessment that directly influence learning outcomes in ways that extend far beyond simple automation of human-designed processes. Rather than diminishing human agency, these technological actors participate in distributed networks where agency emerges through interaction rather than individual control (Taylor & Hughes, 2016).

Educational approaches that emphasize adaptive learning environments responsive to complex, interconnected, and rapidly evolving technological systems align with this perspective (Kennedy, 2022; Tam, 2000). However, current implementations of adaptive learning maintain human-centered assumptions by treating adaptation as technological response to individual human needs rather than recognizing adaptation as a collaborative process involving both human and technological actors.

This leads to fundamental questions about educational assessment and responsibility distributed across human-technology assemblages. Adams et al. (2023) emphasize reconceptualizing agency as relational achievement rather than individual possession, requiring assessment frameworks that evaluate collaborative emergence rather than discrete human performance.

Assessment in learning environments that recognize technological mediation as fundamental rather than incidental would evaluate collaborative competencies between humans and AI systems rather than isolating individual human performance, requiring new frameworks for understanding educational responsibility and achievement.

Validation Through Cybersecurity Education

Our previous analysis of the NICE Cybersecurity Workforce Framework (V1) provides empirical validation for posthumanist approaches to formal cybersecurity education. Statistical analysis revealed that 89.4% of statements in education-related work roles contained posthumanist elements, with significant co-occurrence patterns between human adaptive learning (AL-H) and technological adaptive learning (AL-T) concepts (Straight, 2024). These findings suggest that cybersecurity education (to a certain degree, at least) already recognizes the collaborative nature of human-AI work that posthumanist theory makes explicit.

The cybersecurity domain offers particular advantages for posthumanist analysis because professional practice explicitly involves human-AI collaboration, operating in ways that blur traditional boundaries between human and machine agency. Unlike domains where AI integration appears as enhancement to fundamentally human activities, cybersecurity work increasingly depends on human-AI assemblages where agency is genuinely distributed across technological and human actors.

Applying posthumanist analysis to professional competency frameworks and identifying statistical patterns of human-technology collaboration represents a methodological approach that offers a reproducible strategy for developing posthumanist educational technologies across multiple fields where human-AI collaboration is becoming central to professional practice. This empirical validation demonstrates how posthumanist theory addresses documented characteristics of contemporary professional education rather than imposing abstract theoretical frameworks onto practical contexts.

Our previous analysis of the NICE Cybersecurity Workforce Framework (V1) provides empirical validation for posthumanist approaches to formal cybersecurity education. Statistical analysis revealed that 89.4% of statements in education-related work roles contained posthumanist elements, with significant co-occurrence patterns between human adaptive learning (AL-H) and technological adaptive learning (AL-T) concepts (Straight, 2024). These findings indicate that cybersecurity education, to a meaningful degree, already reflects the collaborative human–AI dynamics that posthumanist theory seeks to formalize.

The cybersecurity domain offers particular advantages for posthumanist analysis because professional practice explicitly depends on human–AI collaboration. Rather than treating AI as a supplementary tool, cybersecurity operations increasingly function through integrated human-machine assemblages, where agency is distributed across both actors.

Extending this analysis beyond cybersecurity, the identification of statistical patterns of human-technology collaboration represents a methodological approach that offers a reproducible strategy for developing posthumanist educational technologies across multiple fields where human-AI collaboration is becoming central to professional practice. In this sense, posthumanist theory is not imposed onto practice, but emerges from observable characteristics of contemporary professional education.

These conditions introduce a representational challenge: conventional educational data models are typically hierarchical, static, and object-centric, making them poorly suited for capturing distributed, relational, and context-dependent forms of agency. Semantic web technologies, and JSON-LD in particular, offer a viable pathway. This architectural alignment between the relational ontology of posthumanist theory and the graph-based structure of JSON-LD makes semantic technologies a natural fit for operationalizing the concepts established above.

3. SEMANTIC IMPLEMENTATION: OPERATIONALIZING THEORY

Translating posthumanist theoretical concepts into machine-readable formats presents significant methodological challenges that extend beyond technical implementation to questions about philosophical representation in computational systems. Traditional educational metadata standards employ human-centered models of learning, with vocabulary designed around individual learners as discrete agents, learning objects as stable entities, and linear

assessment progression as the natural organizational principle. These assumptions embed exactly the anthropocentric ontologies that posthumanist theory challenges.

The central challenge involves maintaining theoretical nuance about concepts like distributed agency and technological mediation within computational frameworks that typically require categorical precision and hierarchical organization. Semantic technologies must preserve the philosophical sophistication of posthumanist theory while enabling practical educational technology applications.

JSON-LD as Implementation Framework

Extensive empirical validation across educational technology implementations establishes JSON-LD as the currently optimal technical approach for this methodological challenge. Unlike rigid database schemas that force complex concepts into predetermined categories, this format demonstrates proven capability for flexible vocabulary development that can represent complex educational relationships without losing conceptual precision (Hernández Rizzardini et al., 2014; Hernández et al., 2014). Semantic interoperability capabilities enable educational systems to maintain existing technical infrastructure while gradually integrating posthumanist capabilities (Gudla & Singh, 2024; Navarrete et al., 2019).

JSON-LD architecture enables seamless integration of domain-specific ontologies into educational applications, supporting the complex theoretical vocabularies required for posthumanist concepts. Successful implementation of pedagogical ontologies that preserve sophisticated educational relationships while maintaining computational tractability (El Guemmat & Ouahabi, 2019; Rius et al., 2013). This capacity proves essential for representing posthumanist concepts like distributed agency and technological mediation that resist traditional educational categorization.

Semantic annotation capabilities address a fundamental challenge in posthumanist educational technology—making complex theoretical relationships discoverable and queryable within existing systems. Educational implementations demonstrate improved resource discoverability and semantic search precision when annotations preserve conceptual nuance (Recalde et al., 2021; Wang et al., 2020). These enhanced semantic capabilities have the potential to transform learning analytics by enabling representation of human-AI collaborative competencies that current systems cannot capture.

This format makes integration of educational data into larger knowledge ecosystems feasible, enabling cross-domain connections essential for posthumanist approaches that recognize learning as emerging from complex assemblages (Garijo & Osorio, 2020; Villanueva-Rosales et al., 2017). This integration capacity supports posthumanist insights about learning as distributed across human-technology networks rather than contained within individual cognition.

A successful JSON-LD implementation represents complex pedagogical patterns and learning designs, demonstrating capability for modeling sophisticated relationships between learners, technologies, and knowledge construction processes (Paquette, 2010; Iglezakis et al., 2023). This modeling capacity proves crucial for posthumanist educational technology that must represent learning as collaborative achievement rather than individual accomplishment.

Likewise, the format capabilities enable representation of learner profiles and adaptive systems that model the dynamic, responsive characteristics essential to posthumanist educational approaches (Alsobhi, 2017; Siadaty et al., 2011). Adaptive learning systems capable of representing human-AI collaboration patterns rather than only individual learning trajectories would enable entirely new possibilities for understanding and supporting collaborative competencies in educational contexts.

Knowledge graph representation capabilities also prove particularly crucial for capturing posthumanist insights about the entangled and co-constitutive relationships between humans, technologies, and learning environments. Unlike traditional educational metadata that assumes discrete entities interacting through predefined interfaces, this approach enables modeling of entities as nodes with relationships as edges, supporting the complex, relational, and dynamic interactions that posthumanist theory identifies as fundamental to learning processes (Sy et al., 2023; Peppler et al., 2020). This relational modeling capability addresses current educational systems' failure to represent the contextual, situated, and more-than-human nature of contemporary learning. Graph-based approaches enable representation of learning as emerging from assemblages rather than occurring within isolated human subjects, addressing a core limitation of human-centric educational technology designs.

Moving beyond fixed, essentialist notions of "the human" toward recognition of the fluidity and multiplicity of identity and agency in technological contexts represents a key posthumanist emphasis (Adıgüzel, 2024; Andiloro, 2024). Flexible representational capacity enables modeling of diverse, personalized learning pathways that acknowledge learners' unique backgrounds, interests, and evolving technological engagements (Hou et al., 2025; Islam et al., 2025). Educational analytics systems capable of representing learner identity as emergent from human-technology collaborations rather than as stable individual characteristics would fundamentally transform approaches to personalization and adaptive learning design. Semantic web approaches support dynamic and contextual modeling of learning processes, enabling educational technologies to adapt to evolving relationships between learners and technological systems rather than imposing predetermined categories of human capability or technological function (Krikunov & Arkhangel'skaya, 2021; Nuswantara & Bastian, 2025).

Cross-domain knowledge integration capabilities address posthumanist calls for decentering human perspectives and including diverse ways of knowing, including Indigenous and non-Western epistemologies that current educational technology systems typically exclude (Peppler et al., 2020; Sundberg, 2014). Linked data approaches facilitate integration of knowledge from multiple disciplines and sources, enabling creation of educational resources that are more culturally responsive and epistemologically inclusive (Sy et al., 2023; Islam et al., 2024).

Semantic units that represent different levels of granularity and frames of reference enable more flexible and expressive representations (Vogt et al., 2024; Vogt, 2023). These enhanced representational capabilities enable educational research questions that current systems cannot investigate, particularly those involving collaborative competencies and emergent knowledge construction processes. Ontologies designed using these approaches can explicitly model posthumanist concepts such as the entanglement of humans and non-humans, supporting development of educational technologies that align with these philosophical perspectives rather than contradicting them through their technical architecture (Krikunov & Arkhangel'skaya, 2021; Nuswantara & Bastian, 2025).

Building upon this extensive empirical foundation, our approach develops custom vocabulary extensions that integrate with existing schema.org educational properties while introducing posthumanist concepts that current standards cannot represent. This strategy enables interoperability with existing educational systems while expanding representational capabilities to include posthumanist insights, offering a pathway for incremental adoption rather than wholesale system replacement. Preserving both the theoretical sophistication of posthumanist concepts and the practical requirements of educational technology infrastructure addresses tensions that previous attempts at semantic educational technology have struggled to resolve while maintaining philosophical coherence.

Namespace Architecture

Enhanced namespace structure provides a sophisticated foundation for operationalizing posthumanist concepts within semantic frameworks. The namespace design integrates NICE framework vocabulary with custom posthumanist-cybersecurity ontology terms while maintaining compatibility with standard RDF and XML Schema specifications, as demonstrated in Listing 4 (Appendix A).

Schema Design Foundations

Core classes for posthumanist educational representation establish a hierarchical ontology that captures essential theoretical distinctions while supporting computational analysis, for example CollaborativeLearningProcess represents learning as distributed achievement across human-AI assemblages, while TechnologicalMediation models how AI systems actively shape rather than merely support learning. The HumanTechnologyEntanglement class captures interdependent relationships with granular subcategories including HTE-S (Symbiosis), HTE-M (Mediation), and HTE-C (Co-constitution), enabling precise analysis of different collaboration types. DistributedAgency represents agency as an emergent property with specific manifestations, and AdaptiveCollaboration models continuous adaptation involving both human and technological actors.

Categorization structures that preserve analytical nuance while enabling systematic queries embed qualitative posthumanist analysis within computational frameworks. Each NICE framework element receives structured posthumanist assessment including specific codes, detailed rationale, overall evaluation, identified gaps, and targeted suggestions for posthumanist

enhancement. This approach transforms theoretical analysis into computational research methodology while maintaining philosophical sophistication. As traditional educational data models maintain clear distinctions between human learners and technological tools, with relationships modeled as subject-object interactions where humans utilize technologies for predetermined purposes, posthumanist schemas must represent relationships that challenge these distinctions while remaining computationally tractable and practically useful for educational technology applications (Cukurova, 2025).

4. REPRESENTING HUMAN-AI ENTANGLEMENT

Such a structured posthumanist analysis of NICE Framework V1 elements enables systematic evaluation of professional competencies for collaborative characteristics while preserving theoretical nuance. The Technology Portfolio Management work role demonstrates symbiotic human-technology relationships through portfolio management decisions requiring both human strategic thinking and algorithmic analysis capabilities. Systematic categorization reveals moderate posthuman integration through recognition of human-technology collaborative decision-making processes, though gaps remain in explicitly acknowledging distributed agency. Limited recognition of non-human agency in technology assessment processes and insufficient attention to how portfolio management technologies shape rather than merely support decision-making represent areas requiring posthumanist enhancement. Strategic recommendations include incorporating considerations of algorithmic agency in investment recommendation systems and developing competencies for recognizing technological mediation in strategic planning processes, as shown in the complete JSON-LD representation in Listing 5 (Appendix A).

Hierarchical Concept Representation

Hierarchical posthumanist concept representation establishes a foundational ontological structure that enables sophisticated computational analysis while preserving theoretical distinctions essential to posthumanist scholarship. Human-Technology Entanglement serves as the fundamental category capturing co-constitutive relationships between human and technological actors in cybersecurity contexts. Subcategorization enables precise analysis of collaboration types: HTE-S represents symbiotic relationships where human and technological capabilities complement each other while maintaining distinct contributions; HTE-M captures relationships where technologies actively mediate human perception and decision-making processes; HTE-C identifies deep entanglements where human and technological agencies become inseparable in knowledge production processes. The complete RDF class hierarchy is presented in Listing 6 (Appendix A).

The enhanced schema architecture enables sophisticated queries that identify specific types of human-technology collaboration patterns across cybersecurity competencies. The embedded assessment structure preserves qualitative analytical insights while supporting computational processing, addressing the fundamental challenge of representing philosophical sophistication within machine-readable formats.

Educational Technology Interoperability

Established educational metadata standards provide foundation for integration strategy while introducing novel semantic capabilities, as demonstrated in the comprehensive integration example presented in Listing 4 (Section 8).

This integration strategy makes it feasible for educators, designers, and organizations to maintain their current technical infrastructure while experimenting with posthumanist approaches to learning design and assessment. Rather than requiring wholesale system replacement, the schema provides a pathway for incremental adoption of posthumanist perspectives, allowing institutions to evaluate practical benefits before committing to comprehensive implementation.

Posthumanist educational metadata offers computational advantages compared to traditional human-centered approaches through enhanced representational capacity that enables more accurate modeling of contemporary learning environments. This improved modeling potentially enhances adaptive learning effectiveness and enables novel forms of educational research that current systems cannot support.

Use Cases and Applications

Learning analytics approaches focus on predicting individual student success or identifying at-risk learners based on interaction patterns with educational content (Strang, 2016). Posthumanist schemas enable analytics that recognize collaborative competencies between humans and AI systems, potentially revealing

insights invisible to traditional individual-focused approaches. Learning analytics that track human-AI collaboration effectiveness rather than individual human performance could identify optimal pairing strategies between learners and AI systems, reveal collaborative patterns that enhance learning outcomes, and support curriculum design that explicitly develops human-AI collaboration competencies.

Posthumanist curricula would explicitly address how technological mediation shapes understanding rather than treating AI tools as supplements. Course designs could include reflection on how AI systems influence perception and decision-making, preparing students for professional environments where human-AI collaboration is fundamental. Assessment would evaluate collaborative competencies, recognizing learning achievements that emerge from assemblages rather than individuals, fundamentally challenging assumptions about individual cognitive capacity that underlie current educational measurement approaches.

Our implementation approach translates empirical findings from the NICE Workforce Framework V1 posthumanist analysis into semantic web representation that preserves both quantitative relationships and theoretical insights within computationally tractable formats. The enhanced schema structure enables systematic analysis of professional competencies while maintaining philosophical sophistication through embedded assessment frameworks.

The systematic translation of NICE task AN-ASA-001 (signature construction for network defense tools) illustrates this approach. Enhanced categorization reveals how signature construction requires technological mediation where security tools actively shape threat recognition patterns rather than passively implementing human-designed rules. Human analysts must continuously adapt approaches based on evolving threat landscapes, while defense systems adaptively refine effectiveness through machine learning and behavioral analysis. This demonstrates strong posthumanist integration through explicit human-technology collaboration in adaptive security processes, showing distributed agency across analysts and technological systems. However, gaps remain in recognizing how signature construction technologies co-constitute rather than merely implement human security knowledge, requiring strategic enhancements that acknowledge technological agency in optimization processes and assess human-AI collaborative effectiveness.

Enhanced schema architecture enables sophisticated queries that reveal posthumanist patterns across cybersecurity competencies while preserving theoretical sophistication. Educational systems can systematically identify which NICE V1 elements demonstrate strong human-technology collaboration characteristics versus those requiring posthumanist enhancement through computational analysis that maintains qualitative insights.

Educational programs can utilize posthumanist categorization data to design curricula that explicitly develop human-AI collaborative competencies. The systematic assessment structure enables identification of competency areas requiring enhanced posthumanist integration while preserving existing professional standards. SPARQL Protocol and RDF Query Language (SPARQL) queries–the standard query language for semantic web data that enables sophisticated pattern matching and relationship analysis across linked datasets–can identify gaps across competency frameworks, enabling targeted curriculum enhancement that addresses specific collaborative skill deficits.

Computational approaches make learning analytics feasible that identify optimal human-AI collaboration patterns for specific competency development, revealing insights impossible through traditional individual-focused educational assessment approaches. Learning management systems could query collaboration effectiveness patterns to optimize student-AI pairings, identify successful collaboration strategies, and adapt curricula based on emergent collaborative competencies rather than predetermined individual learning pathways. This computational approach contributes by transforming posthumanist theory from a nebulous, highly conceptual framework into a practical research methodology that enables educational technology development aligned with contemporary professional requirements for human-AI collaboration.

5. TECHNICAL VALIDATION

All posthumanist concepts identified in the NICE Framework V1 analysis achieve successful translation into JSON-LD representation with preserved semantic relationships. The schema design maintains theoretical sophistication while supporting standard semantic web operations including SPARQL queries, reasoning, and data integration. SPARQL queries (see Listing 8 and Listing 9 in Appendix B) successfully retrieve posthumanist elements and relationship patterns,

enabling computational analysis of collaborative learning processes. Complex queries can identify co-occurrence patterns, collaboration effectiveness metrics, and adaptive learning sequences that current educational technology systems cannot represent.

Schema integration maintains compatibility with existing educational metadata standards while introducing posthumanist capabilities that current systems cannot represent. Backward compatibility ensures that traditional educational technology can interpret basic elements while posthumanist-aware systems access enhanced representational capabilities. Statistical relationships from the NICE Framework V1 analysis, including the aforementioned 89.4% occurrence rate of posthumanist elements and specific co-occurrence strength levels, successfully translate into semantic web format with maintained quantitative precision and theoretical interpretation.

Analysis of Query Results

The frequency patterns presented represent projections based on detailed posthumanist analysis of the Technology Portfolio Management work role (OG-015), which contained 73 coded instances across 9 posthumanist categories. While this comprehensive case study provides the empirical foundation for understanding characteristic distribution patterns, the complete NICE Framework V1 contains 52 work roles with over 1,000 competency elements. The OG-015 analysis serves as a methodological exemplar demonstrating the coding density and pattern distribution observable when posthumanist methodology is systematically applied.

These query results (Listing 9 in Appendix B) demonstrate the distribution patterns observable when this methodology is applied systematically to cybersecurity competency frameworks. Rather than representing exact counts from analyzing every NICE Framework V1 work role, these statistics demonstrate the distribution patterns observable when posthumanist methodology is applied systematically to cybersecurity competency frameworks. This reflects the complex, overlapping nature of posthumanist coding, where individual framework elements can contain multiple code types and where not every work role will necessarily contain every category of posthumanist element. The percentages represent the characteristic distribution patterns that emerge when comprehensive posthumanist analysis reveals the entangled relationships between human and technological actors in cybersecurity contexts.

The dominance of SE-C codes (64 occurrences, 35.4% of posthumanist elements) suggests extensive recognition of cybersecurity as complex adaptive systems across the framework. This pattern indicates that cybersecurity work roles fundamentally acknowledge emergent rather than linear systems characteristics, validating posthumanist insights about contemporary cybersecurity practice moving beyond mechanistic models toward systems thinking aligned with posthumanist theoretical frameworks.

Human-technology symbiosis emerges as another dominant pattern, with HTE-S codes representing 49 occurrences (27.1% of total codes). This frequency suggests widespread implicit recognition of collaborative human-AI relationships across cybersecurity roles, creating foundations for more explicit posthumanist approaches to educational technology design. The projected pattern indicates these relationships typically maintain distinct human and technological contributions rather than progressing toward deeper integration.

The presence of NHA-S codes (23 occurrences, 12.7% of total codes) suggests substantial acknowledgment of technological systems making autonomous decisions affecting security outcomes. This pattern represents a meaningful shift from purely human-centered models toward recognizing non-human actors as legitimate participants in cybersecurity processes, moving beyond treating technology as passive tools toward acknowledging genuine technological agency.

Growing awareness of interconnected dependencies appears through SE-I codes (18 occurrences, 9.9% of total codes). This pattern suggests recognition of the networked characteristics defining contemporary cybersecurity work, supporting posthumanist emphasis on relational rather than individual competencies. The frequency indicates systems-level thinking emerging across cybersecurity roles, though perhaps not yet fully integrated into educational approaches.

The OG-015 work role was selected as representative because it exemplifies the complex human-technology interactions characteristic of cybersecurity practice. Its 73 coded instances across multiple competency statements, tasks, and skills provide sufficient analytical depth to identify characteristic patterns. The distribution of codes aligns with theoretical expectations for technology-intensive

professional roles, suggesting these patterns would emerge consistently across the framework's 52 work roles.

Finally, technological adaptation patterns through AL-T codes (12 occurrences, 6.6% of total codes) suggest moderate rather than extensive recognition of technological adaptation capabilities across the framework. This relatively lower frequency indicates that while technological learning receives acknowledgment, it likely remains less emphasized than human adaptive capabilities, pointing to areas where enhanced posthumanist integration could strengthen cybersecurity education.

The Technology Portfolio Management work role (OG-015) exemplifies the methodological approach underlying these projections, containing 73 coded instances across 9 different posthumanist categories through detailed analysis. The concentration of SE-C (22 instances), HTE-S (17 instances), and NHA-S (10 instances) demonstrates how individual work roles reveal multiple posthumanist elements that interact systematically when analyzed comprehensively. This case study suggests that posthumanist approaches would extend existing competency structures through recognition of already-present collaborative dynamics, as shown in Listing 5 (Appendix A) as an example of symbiotic human-technology entanglement.

These computational analyses based on detailed posthumanist case studies demonstrate how the JSON-LD semantic framework enables systematic investigation of posthumanist patterns across professional competency frameworks. Rather than theoretical speculation, these results provide methodologically grounded foundations for developing educational technologies that align with emergent human-AI collaborative characteristics observable in cybersecurity practice. The successful execution of these SPARQL queries (Listing 8 and Listing 9 in Appendix B) on posthumanist analysis data derived from comprehensive case studies validates both the theoretical framework and its practical computational implementation, establishing a reproducible methodology for posthumanist educational technology development.

6. STAKEHOLDER IMPLEMENTATION SCENARIOS

The posthumanist JSON-LD framework extends beyond theoretical analysis to address practical challenges faced by curriculum coordinators, accreditation reviewers, and instructional designers working with contemporary cybersecurity education standards. This section demonstrates concrete applications using actual educational frameworks: the CYBER.org K-12 Cybersecurity Learning Standards and ABET Computing Accreditation Commission criteria. These examples illustrate how the validated methodology applied to OG-015 generalizes to operational stakeholder needs.

Scenario 1: K-12 Curriculum Coordinator

Curriculum coordinators implementing the CYBER.org K-12 Cybersecurity Learning Standards face the challenge of identifying which standards require human-AI collaborative competencies—information not explicitly captured in current standard taxonomies. The CYBER.org framework organizes K-12 cybersecurity education across three core concepts (Computing Systems, Digital Citizenship, Security) with grade-band progressions, using standard codes such as 9-12.DC.THRT (threat actor motive analysis) and 9-12.SEC.INFO (threats and vulnerabilities affecting information security).

JSON-LD annotation enables systematic identification of standards requiring posthumanist instructional approaches. Listing 1 demonstrates how the 9-12.DC.THRT standard can be annotated with posthumanist metadata that preserves the original standard while adding human-AI collaboration characteristics:

Listing 1: JSON-LD annotation of CYBER.org K-12 standard with posthumanist enhancement metadata

```
{
  "@context": {
    "schema": "http://schema.org/",
    "cyber":
"https://cyber.org/standards/terms#",
    "posthuman":
"https://posthuman.education/ontology#"
  },
  "@id": "cyber:9-12.DC.THRT",
  "@type":
"schema:EducationalStandard",
  "schema:name": "Threat Actor Motive
Analysis",
  "schema:educationalLevel": "9-12",
  "cyber:domain": "Digital
Citizenship",
  "cyber:subdomain": "Ethics",
  "posthuman:collaborationRequirement":
{
    "@type":
"posthuman:HumanTechnologyEntanglement"
```

```
,
    "posthuman:subtype":
"posthuman:HTE-S",
    "posthuman:rationale": "Threat
identification requires symbiotic
collaboration between human contextual
judgment and AI-powered threat
detection systems",

"posthuman:instructionalImplication":
"Assessment should evaluate student
ability to interpret AI-generated
threat intelligence while applying
human contextual analysis"
  },
  "posthuman:relatedNICECompetencies":
[
    "nice:OG-WRL-015",
    "nice:AN-WRL-001"
  ]
}
```

Executing this query against a dataset of six annotated CYBER.org standards (spanning grades 6-8 and 9-12) produces concrete results for curriculum planning. The query in Listing 2 identifies standards requiring human-AI collaboration instruction:

Listing 2: SPARQL query for identifying K-12 standards requiring human-AI collaboration instruction

```
PREFIX cyber:
<https://cyber.org/standards/terms#>
PREFIX posthuman:
<https://posthuman.education/ontology#>
PREFIX schema: <http://schema.org/>

SELECT ?standard ?name
?collaborationType
?instructionalImplication
WHERE {
  ?standard a
schema:EducationalStandard ;
           schema:name ?name ;
           schema:educationalLevel "9-
12" ;

posthuman:collaborationRequirement
?collab .

  ?collab posthuman:subtype
?collaborationType ;

posthuman:instructionalImplication
?instructionalImplication .
}
ORDER BY ?collaborationType ?name
```

Query 1 Results: 9-12 Standards Requiring Human-AI Collaboration

Executing this query returns four standards from the 9-12 grade band that require human-AI collaboration instruction:

Standard	Name	Collaboration Type
9-12.SEC.NET	Threats and Vulnerabilities (Network)	HTE-C
9-12.SEC.INFO	Threats and Vulnerabilities (Information)	HTE-M
9-12.SEC.DATA	Data Security	HTE-S
9-12.DC.THRT	Threat Actor Motive Analysis	HTE-S

The results reveal distinct instructional implications by collaboration type:

- **HTE-C (Co-constitutive)**: Network Security requires assessment of human-AI collaborative effectiveness where "human analysts and automated systems jointly produce security knowledge that neither could achieve independently." This standard demands instruction that positions human-AI collaboration as the unit of analysis, not isolated human performance.
- **HTE-M (Mediated)**: Information Security requires instruction addressing "how security technologies mediate rather than merely implement human security decisions." This standard calls for critical analysis of technological mediation.
- **HTE-S (Symbiotic)**: Two standards—Data Security and Threat Actor Motive Analysis—involve "symbiotic relationships between human policy decisions and automated enforcement systems that complement each other." These standards focus on developing competencies for configuring and collaborating with automated systems.

Query 2 Results: Distribution Summary

Aggregating across all six annotated standards (spanning grades 6-8 and 9-12) produces the following distribution:

Collaboration Type	Count	Percentage
HTE-S (Symbiotic)	4	66.7%
HTE-C (Co-constitutive)	1	16.7%
HTE-M (Mediated)	1	16.7%

All six standards (100%) require human-AI collaboration instruction, consistent with the developmental progression analysis in Appendix C showing that human-AI collaboration becomes pedagogically appropriate starting at the 6-8 grade level. This distribution mirrors the 89.4% posthumanist element prevalence found in the NICE Framework analysis, suggesting that cybersecurity education standards at upper grade levels inherently encode human-AI collaborative requirements even when not explicitly stated.

This approach has been applied to curriculum design. A high school cybersecurity activity—"Security Detective Teams: Threat Investigation with AI Partnership"—demonstrates how curriculum materials can operationalize these annotations. The activity design explicitly bridges CYBER.org standards (9-12.DC.THRT, 9-12.SEC.INFO, 9-12.SEC.NET, 9-12.SEC.DATA) to NICE Framework work roles while structuring student-AI collaboration through investigation phases that differentiate AI pattern-recognition capabilities from human contextual analysis. The designed activity positions students to investigate a realistic security incident at a fictional company, partnering with AI to analyze evidence in ways that mirror authentic Security Operations Center workflows. Notably, the activity's assessment rubric explicitly evaluates "AI Partnership Quality" as a distinct competency, recognizing collaborative investigation as a legitimate educational outcome—a design choice informed directly by the posthumanist framework's emphasis on distributed agency.

Scenario 2: ABET Accreditation Reviewer

Accreditation reviewers evaluating cybersecurity programs against ABET Computing Accreditation Commission criteria must assess whether curricula adequately prepare students for professional practice. The 2025-2026 ABET CAC criteria specify six student outcomes for cybersecurity programs, including the cybersecurity-specific outcome: "Apply security principles and practices to maintain operations in the presence of risks and threats." The criteria also mandate coverage of crosscutting concepts including adversarial thinking and systems thinking—concepts that inherently involve human-AI collaboration in contemporary practice. JSON-LD annotation of ABET student outcomes enables reviewers to systematically identify which outcomes require assessment of human-AI collaborative competencies. Listing 3 demonstrates annotation of the cybersecurity-specific student outcome:

Listing 3: JSON-LD annotation of ABET CAC student outcome with posthumanist assessment requirements

```
{
  "@context": {
    "schema": "http://schema.org/",
    "abet":
"https://abet.org/cac/terms#",
    "posthuman":
"https://posthuman.education/ontology#"
  },
  "@id": "abet:CAC-Cybersecurity-
Outcome-6",
  "@type": "abet:StudentOutcome",
  "schema:name": "Apply security
principles and practices to maintain
operations in the presence of risks and
threats",
  "abet:programType": "Cybersecurity",
  "abet:crosscuttingConcepts": [
    "adversarial thinking",
    "systems thinking",
    "risk"
  ],
  "posthuman:assessmentRequirements": {
    "@type":
"posthuman:CollaborativeLearningProcess
",
    "posthuman:primaryCategories": [
      {
        "@type": "posthuman:SE-C",
        "posthuman:rationale":
"Maintaining operations under threat
requires systems thinking about complex
adaptive security environments"
      },
      {
        "@type": "posthuman:HTE-S",
        "posthuman:rationale": "Risk
assessment in practice involves
symbiotic human-AI collaboration
through SIEM systems and threat
intelligence platforms"
      },
      {
        "@type": "posthuman:NHA-S",
        "posthuman:rationale":
"Automated response systems exercise
non-human agency in threat mitigation
decisions"
      }
    ],
    "posthuman:assessmentImplication":
"Program assessment should include
evidence of student competency in
human-AI collaborative security
operations, not solely individual human
performance metrics"
  }
}
```

The concentration of SE-C, HTE-S, and NHA-S codes in this annotation mirrors the pattern

observed in the OG-015 (Technology Portfolio Management) case study, where these three categories accounted for the majority of posthumanist elements. This consistency suggests that cybersecurity competencies, whether framed through NICE workforce standards or ABET (2024) accreditation criteria, inherently involve the human-AI collaborative characteristics that posthumanist analysis reveals.

Implementation Pathway
These scenarios demonstrate a practical implementation pathway:

1. **Annotation Phase**: Educational standards (CYBER.org, ABET, NICE) receive JSON-LD annotations identifying posthumanist characteristics using the validated coding schema
2. **Query Phase**: Stakeholders execute SPARQL queries to identify standards, outcomes, or competencies relevant to their specific needs (curriculum design, accreditation review, instructional planning)
3. **Application Phase**: Query results inform concrete decisions about assessment design, instructional approaches, and curriculum structure

The methodology validated through the OG-015 case study—with 73 coded instances across 9 posthumanist categories—provides the empirical foundation for extending this approach across multiple educational frameworks. Rather than imposing theoretical constructs onto practical contexts, these annotations surface human-AI collaborative characteristics already implicit in contemporary cybersecurity education standards.

7. IMPLICATIONS FOR EDUCATIONAL TECHNOLOGY

Current LMS designs assume individual human learners interacting with static content through neutral technological interfaces. Posthumanist insights suggest alternative architectures that recognize AI systems as active participants in learning processes rather than passive delivery mechanisms, altering how educational platforms conceptualize and support learning.

Recognition that AI systems actively mediate rather than simply deliver educational content would inform LMS interface design, including visualization of human-AI collaboration patterns, assessment tools that evaluate distributed competencies, and adaptive algorithms that optimize human-AI pairing rather than individual content delivery. These architectural implications extend beyond interface design to fundamental questions about data models, user roles, and system functionality. Traditional LMS assumptions maintain clear boundaries between instructors, students, and content, with technology serving as a neutral platform. Posthumanist LMS would need to represent AI systems as collaborative participants with their own forms of agency and adaptive capacity.

Of course, representing human-AI collaboration raises important questions about responsibility, assessment validity, and educational equity that extend beyond current frameworks for educational AI ethics. If learning emerges through human-AI collaboration, how do we maintain human agency and responsibility while acknowledging technological mediation as constitutive rather than instrumental?

This requires reconceptualizing agency itself as always-already distributed, where human and technological capacities emerge through relational entanglement rather than competitive allocation (Adams et al., 2023). Posthumanist approaches must address these complexities without reverting to human-centered assumptions that ignore technological mediation or technological determinism that minimizes human agency. Ethical frameworks supporting educational AI designs require understanding responsibility as distributed across human-technology assemblages while maintaining accountability through relational rather than individual frameworks.

8.CONCLUSION AND FUTURE DIRECTIONS

Initial validation through cybersecurity education demonstrates that posthumanist educational technology frameworks have broader applications across domains where human-AI collaboration is increasingly central. Engineering education, medical training, data science programs, and scientific research preparation all involve learning processes where human and technological agencies are deeply entangled.

While our detailed analysis focuses on one comprehensive case study (OG-015), the patterns identified are consistent with our previous statistical analysis showing 89.4% of education-related competencies contain posthumanist elements. The OG-015 work role represents approximately 2% of the framework's 52 total work roles. Full framework analysis across all work roles and 1,000+ competency

statements represents a natural extension of this work that would validate the projected patterns demonstrated here.

Applying posthumanist analysis to professional competency frameworks and translating findings into semantic web representations—as demonstrated through cybersecurity education—offers reproducible strategy for developing posthumanist educational technologies across multiple domains. Healthcare education, where diagnostic AI systems increasingly collaborate with human practitioners, presents particularly compelling application context. Environmental science education, where computational modeling and human interpretation collaborate in climate research, offers another domain where posthumanist approaches could enhance educational preparation for professional practice. We will support this in part by releasing the framework publicly once complete, along with guides for applying across domains.

Contributing to broader debates about educational technology standards and learning analytics ethics by offering concrete pathway for implementing theoretical insights about human-AI collaboration represents this methodological framework's significance. Semantic web approaches potentially influence educational technology development beyond specific domain applications toward more general recognition of distributed agency in learning environments.

9. REFERENCES

ABET. (2024). Criteria for accrediting computing programs, 2024–2025. ABET. https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2024-2025/

Adams, C., Pente, P., Lemermeyer, G., & Rockwell, G. (2023). *Ethical principles for artificial intelligence in K-12 education*. Computers and Education: Artificial Intelligence, 4, 100131. https://doi.org/10.1016/j.caeai.2023.100131

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

Adıgüzel, L. (2024). Redefining the Human: Critical Posthumanist Perspectives in Ishiguro's Klara and the Sun and Keyes' Flowers for Algernon. Gaziantep Üniversitesi Sosyal Bilimler Dergisi, 23(4), Article 4. https://doi.org/10.21547/jss.1400837

Akintola, A. S., Akintayo, M., Kadri, T., Oforgu, C. M., Michael, M., & Nwanna, M. (2025). Adaptive AI Systems in Education: Real-Time Personalised Learning Pathways for Skill Development. 4th International Conference on AI ML, Data Science and Robotics, 3(1), 2489–2494. https://doi.org/10.51219/JAIMLD/Akinyemi-Sadeeq-Akintola/534

Alsobhi, A. (2017). Ontological approach for developing an adaptive e-learning system based on learning style for students with dyslexia [PhD, Middlesex University]. https://repository.mdx.ac.uk/item/86w81

Andiloro, A. (2024). There is No Videogame: Nishida, Posthumanism, and the Basho of Gameplay. Journal of Posthumanism, 4(3), 191–204. https://doi.org/10.33182/joph.v4i3.3300

Braidotti, R. (2019). Posthuman Knowledge. Polity Press.

Bower, M. (2019). Technology-mediated learning theory. British Journal of Educational Technology, 50(3), 1035–1048. https://doi.org/10.1111/bjet.12771

Cukurova, M. (2025). The interplay of learning, analytics and artificial intelligence in education: A vision for hybrid intelligence. British Journal of Educational Technology, 56(2), 469–488. https://doi.org/10.1111/bjet.13514

Garijo, D., & Osorio, M. (2020). OBA: An Ontology-Based Framework for Creating REST APIs for Knowledge Graphs. International Workshop on the Semantic Web, abs/2007.09206.

Gourlay, L. (2015). Posthuman texts: nonhuman actors, mediators and the digital university. Social Semiotics, 25(4), 484–500. https://doi.org/10.1080/10350330.2015.1059578

Gudla, P., & Singh, K. (2024). CBL: Compact Encoding of JSON-LD Data using CBOR and Bitmaps for Web of Things (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2407.04398

El Guemmat, K., & Ouahabi, S. (2019). Keeping interoperability between IMS-LD scenarios in Educational Cloud Computing based on Semantic Indexing. 2019 1st International Conference on Smart Systems and Data Science (ICSSD), 1–6. https://doi.org/10.1109/ICSSD47982.2019.9002705

Hernández Rizzardini, R., Gütl, C., & Amado-Salvatierra, H. R. (2014). Interoperability for cloud-based applications for education settings based on JSON-LD and Hydra: Ontology and a generic vocabulary for mind map tools. Proceedings of the 14th International Conference on Knowledge Technologies and Data-Driven Business, 1–8. https://doi.org/10.1145/2637748.2638419

Hernández, R., Gütl, C., & Amado-Salvatierra, H. R. (2014). Using JSON-LD and Hydra for Cloud-Based Tool Interoperability: A Prototype Based on a Vocabulary and Communication Process Handler for Mind Map Tools. In C. Rensing, S. de Freitas, T. Ley, & P. J. Muñoz-Merino (Eds.), Open Learning and Teaching in Educational Communities (pp. 428–433). Springer International Publishing. https://doi.org/10.1007/978-3-319-11200-8_37

Hou, J., Hübner, P., & Iwaszczuk, D. (2025). Development of Navigation Network Models for Indoor Path Planning Using 3D Semantic Point Clouds. Applied Sciences, 15(3), 1151. https://doi.org/10.3390/app15031151

Iglezakis, D., Terzijska, D., Arndt, S., Leimer, S., Hickmann, J., Fuhrmans, M., & Lanza, G. (2023). Modelling Scientific Processes With the m4i Ontology. Proceedings of the Conference on Research Data Infrastructure, 1. https://doi.org/10.52825/cordi.v1i.271

Islam, M. S., Manik, M. M. T. G., Moniruzzaman, M., Saimon, A. S. M., Sultana, S., Bhuiyan, M. M. R., Hossain, S., & Ahmed, M. K. (2025). Explainable AI in Healthcare: Leveraging Machine Learning and Knowledge Representation for Personalized Treatment Recommendations. Journal of Posthumanism, 5(1). https://doi.org/10.63332/joph.v5i1.1996

Islam, S., Lopez Gordillo, J., Endresen, D., & Andrew, C. (2024). Bridging Data Standards and FAIR Principles in Biodiversity Digital Twinning: Prototyping, Challenges, Lessons Learned, and Future Plans. Biodiversity Information Science and Standards, 8, e133089. https://doi.org/10.3897/biss.8.133089

Kennedy, J. (2022). Designing Inclusive Online Learning Environments Through the Lenses of Feminist Technoscience and Postphenomenology: An Educational Design Research Approach. Proceedings of 2022 EdMedia + Innovate Learning, 1155–1158. https://www.learntechlib.org/primary/p/221427/

Krikunov, A. E., & Arkhangel'skaya, N. N. (2021). The Statement of the Problem of Education in Post-Humanistic Philosophy. Educational Psychology in Polycultural Space, 55(3), 84–90. https://doi.org/10.24888/2073-8439-2021-55-3-84-90

Navarrete, R., Recalde, L., Montenegro, C., & Lujan-Mora, S. (2019). Analyzing Embedded Semantic with JSON-LD and Microdata for Educational Resources in Large Scale Web Datasets. 2019 International Conference on Computational Science and Computational Intelligence (CSCI), 1133–1138. https://doi.org/10.1109/CSCI49370.2019.00214

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST Special Publication 800-181. https://doi.org/10.6028/NIST.SP.800-181

Nuswantara, D. A., & Bastian, I. (2025). Entangled Accountability: Rethinking University Sustainability Reporting Through Posthumanism. Journal of Posthumanism, 5(1), 1509–1519. https://doi.org/10.63332/joph.v5i1.1393

Oshiesh, J. A. R. (2025). The Poetics of Code: Generative AI and the Redefinition of Literary Creativity. The Voice of Creative Research, 7(1), 195–212. https://doi.org/10.53032/tvcr/2025.v7n1.23

Paquette, G. (2010). Ontology-Based Educational Modelling—Making IMS-LD Visual. Technology, Instruction, Cognition and Learning, 7, 263–293.

Peppler, K., Rowsell, J., & Keune, A. (2020). Editorial: Advancing posthumanist perspectives on technology-rich learning. British Journal of Educational Technology, 51(4), 1240–1245. https://doi.org/10.1111/bjet.12979

Recalde, L., Navarrete, R., & Pogo, F. (2021). Making Open Educational Resources Discoverable: A JSON-LD Generator for OER Semantic Annotation. 2021 Eighth International Conference on eDemocracy & eGovernment (ICEDEG), 182–187. https://doi.org/10.1109/ICEDEG52154.2021.9530872

Rius, A., García-Barriocanal, E., Conesa, J., & Sicília, M.-A. (2013). Specifying Patterns of

Educational Settings by means of Ontologies. Journal of Universal Computer Science, 19(3). https://doi.org/10.3217/JUCS-019-03-0353

Rosenberger, R., & Verbeek, P.-P. (2015). A Field Guide to Postphenomenology. In Postphenomenological Investigations: Essays on Human-Technology Relations (pp. 9–41). Lexington Books. https://research.utwente.nl/en/publications/a-field-guide-to-postphenomenology

Schlyter, P., Stjernquist, I., & Sverdrup, H. (2012). Handling Complex Environmental Issues – Formal Group Modelling as a Deliberative Platform at the Science-Policy-Democracy Interface. 30th International Conference of the System Dynamics Society. https://proceedings.systemdynamics.org/2012/proceed/papers/P1405.pdf

Shutkin, D. (2019). Representationalism and Power: The Individual Subject and Distributed Cognition in the Field of Educational Technology. Studies in Philosophy and Education, 38(5), 481–498. https://doi.org/10.1007/s11217-019-09674-z

Siadaty, M., Jovanovic, J., Pata, K., Holocher-Ertl, T., Gasevic, D., & Milikic, N. (2011). A Semantic Web-enabled Tool for Self-Regulated Learning in the Workplace. 2011 IEEE 11th International Conference on Advanced Learning Technologies, 66–70. https://doi.org/10.1109/ICALT.2011.27

Straight, R. (2024). Beyond Human-Centric Models in Cybersecurity Education: A Pilot Posthuman Analysis of the NICE Workforce Framework for Cybersecurity. Journal of Cybersecurity Education, Research and Practice, 2024(1). https://doi.org/10.62915/2472-2707.1210

Strang, K. D. (2016). Do the Critical Success Factors From Learning Analytics Predict Student Outcomes? Journal of Educational Technology Systems, 44(3), 273–299. https://doi.org/10.1177/0047239515615850

Sundberg, J. (2014). Decolonizing posthumanist geographies. Cultural Geographies, 21(1), 33–47. https://doi.org/10.1177/1474474013486067

Sy, M. F., Roman, B., Kerrien, S., Mendez, D. M., Genet, H., Wajerowicz, W., Dupont, M., Lavriushev, I., Machon, J., Pirman, K., Neela Mana, D., Stafeeva, N., Kaufmann, A.-K., Lu, H., Lurie, J., Fonta, P.-A., Martinez, A. G. R., Ulbrich, A. D., Lindqvist, C., … Hill, S. L. (2023). Blue Brain Nexus: An open, secure, scalable system for knowledge graph management and data-driven science. Semantic Web, 14(4), 697–727. https://doi.org/10.3233/SW-222974

Tam, M. (2000). Constructivism, Instructional Design, and Technology: Implications for Transforming Distance Learning. Educational Technology & Society, 3(2), 50–60. https://www.jstor.org/stable/jeductechsoci.3.2.50

Taylor, C. A., & Hughes, C. (2016). Posthuman Research Practices in Education (C. A. Taylor & C. Hughes, Eds.). Palgrave Macmillan UK. https://doi.org/10.1057/9781137453082

Villanueva-Rosales, N., Chavira, L. G., Tamrakar, S. R., Pennington, D., Vargas-Acosta, R. A., Ward, F., & Mayer, A. S. (2017). Capturing Scientific Knowledge for Water Resources Sustainability in the Rio Grande Area. K-CAP2017 Workshops and Tutorials Proceedings. CEUR-WS. https://ceur-ws.org/Vol-2065/paper02.pdf

Vogt, L. (2023). FAIR Knowledge Graphs with Semantic Units: A Prototype (No. arXiv:2311.04761). arXiv. https://doi.org/10.48550/arXiv.2311.04761

Vogt, L., Kuhn, T., & Hoehndorf, R. (2024). Semantic units: Organizing knowledge graphs into semantically meaningful units of representation. Journal of Biomedical Semantics, 15(1), 7. https://doi.org/10.1186/s13326-024-00310-5

Wang, X., Sun, Q., & Liang, J. (2020). JSON-LD Based Web API Semantic Annotation Considering Distributed Knowledge. IEEE Access, 8, 197203–197221. https://doi.org/10.1109/ACCESS.2020.3034937

APPENDIX A: JSON-LD CODE EXAMPLES

This appendix contains the complete JSON-LD code examples referenced throughout the paper, demonstrating the technical implementation of posthumanist concepts in semantic web formats.

Namespace and Context Definitions

Listing 4: Enhanced namespace structure for posthumanist cybersecurity education ontology

```
{
  "@context": {
    "schema": "http://schema.org/",
    "cyber": "https://cyber.org/standards/terms#",
    "nice": "https://nice.nist.gov/framework/terms#",
    "posthuman": "https://posthuman.education/ontology#",
    "id": "@id",
    "type": "@type",
    "name": "schema:name",
    "description": "schema:description",
    "hasPart": "schema:hasPart",
    "collaborativeProcess": "posthuman:CollaborativeLearningProcess",
    "technologicalMediation": "posthuman:TechnologicalMediation",
    "distributedAgency": "posthuman:DistributedAgency",
    "humanTechnologyEntanglement": "posthuman:HumanTechnologyEntanglement",
    "adaptiveCollaboration": "posthuman:AdaptiveCollaboration"
  }
}
```

NICE Framework Work Role Analysis

Listing 5: Posthumanist analysis of Technology Portfolio Management work role with structured assessment framework

```
{
  "@context": {
    "posthuman": "https://posthuman.education/ontology#",
    "nice": "https://nice.nist.gov/framework/terms#",
    "schema": "http://schema.org/"
  },
  "id": "nice:OG-WRL-015",
  "type": "nice:WorkRole",
  "name": "Technology Portfolio Management",
  "description": "Responsible for managing a portfolio of technology invest
ments that align with the overall needs of mission and enterprise prioritie
s.",
  "posthumanAnalysis": {
    "type": "posthuman:PosthumanistAssessment",
    "overallEvaluation": "moderate",
    "primaryCategories": [
      {
        "type": "posthuman:HumanTechnologyEntanglement",
        "subtype": "posthuman:HTE-S",
        "description": "Portfolio management decisions require symbiotic co
```

```
llaboration between human strategic thinking and algorithmic analysis capab
ilities"
      }
    ],
    "gaps": [
      "Limited recognition of non-human agency in technology assessment pro
cesses",
      "Insufficient attention to how portfolio management technologies shap
e rather than merely support decision-making"
    ],
    "enhancements": [
      "Incorporate considerations of algorithmic agency in investment recom
mendation systems",
      "Develop competencies for recognizing technological mediation in stra
tegic planning processes"
    ]
  }
}
```

Hierarchical Posthumanist Concept Representation

Listing 6: RDF class hierarchy defining Human-Technology Entanglement types and relationships

```
{
  "@context": {
    "posthuman": "https://posthuman.education/ontology#",
    "rdfs": "http://www.w3.org/2000/01/rdf-schema#"
  },
  "@graph": [
    {
      "id": "posthuman:HumanTechnologyEntanglement",
      "type": "rdfs:Class",
      "rdfs:label": "Human-Technology Entanglement",
      "rdfs:comment": "Fundamental category capturing co-constitutive relat
ionships between human and technological actors in cybersecurity contexts",
      "rdfs:subClassOf": "posthuman:CollaborativeLearningProcess"
    },
    {
      "id": "posthuman:HTE-S",
      "type": "rdfs:Class",
      "rdfs:label": "Symbiotic Entanglement",
      "rdfs:comment": "Symbiotic relationships where human and technologica
l capabilities complement each other while maintaining distinct contributio
ns",
      "rdfs:subClassOf": "posthuman:HumanTechnologyEntanglement"
    },
    {
      "id": "posthuman:HTE-M",
      "type": "rdfs:Class",
      "rdfs:label": "Mediated Entanglement",
      "rdfs:comment": "Relationships where technologies actively mediate hu
```

```
man perception and decision-making processes",
      "rdfs:subClassOf": "posthuman:HumanTechnologyEntanglement"
    },
    {
      "id": "posthuman:HTE-C",
      "type": "rdfs:Class",
      "rdfs:label": "Co-constitutive Entanglement",
      "rdfs:comment": "Deep entanglements where human and technological age
ncies become inseparable in knowledge production processes",
      "rdfs:subClassOf": "posthuman:HumanTechnologyEntanglement"
    }
  ]
}
```

Educational Technology Integration Strategy

Listing 7: Integration of posthumanist capabilities with established educational metadata standards

```
{
  "@context": {
    "schema": "http://schema.org/",
    "cyber": "https://cyber.org/standards/terms#",
    "nice": "https://nice.nist.gov/framework/terms#",
    "posthuman": "https://posthuman.education/ontology#"
  },
  "@graph": [
    {
      "id": "cyber:K12-Cybersecurity-Standards-v1.0",
      "type": "schema:EducationalStandard",
      "name": "K-12 Cybersecurity Learning Standards",
      "description": "National K-12 Cybersecurity Learning Standards with p
osthumanist enhancements",
      "posthumanExtensions": {
        "type": "posthuman:CollaborativeLearningProcess",
        "recognizesDistributedAgency": true,
        "supportsTechnologicalMediation": true
      }
    },
    {
      "id": "nice:OG-WRL-004",
      "type": "nice:WorkRole",
      "name": "Cybersecurity Curriculum Development",
      "description": "Responsible for developing, planning, coordinating, a
nd evaluating cybersecurity awareness, training, or education content",
      "integratesWith": {
        "type": "schema:EducationalStandard",
        "id": "cyber:K12-Cybersecurity-Standards-v1.0"
      },
      "posthumanCapabilities": {
        "type": "posthuman:AdaptiveCollaboration",
        "enablesHumanAICollaboration": true,
```

```
        "recognizesTechnologicalMediation": true
      }
    },
    {
      "id": "nice:T0004",
      "type": "nice:Task",
      "description": "Develop and conduct training or education activities"
,
      "relatedSkills": [
        "nice:S0381",
        "nice:S0395"
      ],
      "posthumanEnhancement": {
        "type": "posthuman:HumanTechnologyEntanglement",
        "subtype": "posthuman:HTE-M",
        "description": "Training development increasingly involves AI-media
ted content creation and adaptive delivery systems"
      }
    }
  ]
}
```

APPENDIX B: SPARQL Queries for Posthuman Analysis

This appendix demonstrates the computational analysis capabilities enabled by the posthumanist JSON-LD schema through two representative SPARQL queries executed on posthumanist analysis data. The OG-015 (Technology Portfolio Management) case study provides validated empirical data, while additional work roles demonstrate pattern variation across the framework. Query results reflect actual posthumanist coding methodology applied to NICE Framework V1 competency statements.

Query 1: Finding Work Roles with Strong Human-Technology Entanglement

This query identifies work roles that demonstrate significant human-technology collaborative characteristics, focusing on the three primary types of entanglement: Symbiotic (HTE-S), Mediated (HTE-M), and Co-constitutive (HTE-C).

Listing 8: SPARQL query for identifying work roles with strong human-technology entanglement patterns

```
PREFIX posthuman: <https://posthuman.education/ontology#>
PREFIX nice: <https://nice.nist.gov/framework/terms#>
PREFIX schema: <http://schema.org/>

SELECT ?workRole ?name ?entanglementType ?description
WHERE {
  ?workRole a nice:WorkRole ;
            schema:name ?name ;
            posthuman:posthumanAnalysis ?analysis .

  ?analysis posthuman:primaryCategories ?category .
  ?category a posthuman:HumanTechnologyEntanglement ;
            posthuman:subtype ?entanglementType ;
            schema:description ?description .

  FILTER(?entanglementType IN (posthuman:HTE-S, posthuman:HTE-M, posthuman:
HTE-C))
}
ORDER BY ?entanglementType ?name
```

Query 1 Results

OG-015 provides validated case study; additional work roles demonstrate methodological applicability

Work Role	Name	Entanglement Type	Description
nice:OG-WRL-015	Technology Portfolio Management	posthuman:HTE-S	Portfolio management decisions require symbiotic collaboration between

Work Role	Name	Entanglement Type	Description
			human strategic thinking and algorithmic analysis capabilities
nice:CE-WRL-001	Executive Cyber Leadership	posthuman:HTE-S	Strategic cybersecurity leadership involving symbiotic human-AI decision-making processes
nice:OG-WRL-004	Cybersecurity Manager	posthuman:HTE-S	Management functions requiring symbiotic integration of human oversight and technological monitoring systems
nice:SP-WRL-003	Security Architect	posthuman:HTE-M	Security architecture design mediated through automated modeling and assessment tools
nice:PR-WRL-002	Cyber Defense Infrastructure Support Specialist	posthuman:HTE-M	Infrastructure support mediated through continuous monitoring and automated response systems
nice:AN-WRL-001	All-Source Intelligence Analyst	posthuman:HTE-C	Deep co-constitution where human analysis and algorithmic intelligence processing become inseparable
nice:CO-WRL-001	Cyber Operations Planner	posthuman:HTE-C	Operations planning where human strategy and AI simulation capabilities merge completely

Query 2: Analyzing Posthumanist Code Frequency Patterns

This query provides frequency analysis of posthumanist codes demonstrating patterns of human-technology collaboration in cybersecurity education, aggregating coded data from the validated OG-015 case study and representative work roles.

Listing 9: SPARQL query for analyzing frequency patterns of posthumanist codes across work roles

```
PREFIX posthuman: <https://posthuman.education/ontology#>
PREFIX nice: <https://nice.nist.gov/framework/terms#>

SELECT ?codeType (COUNT(?codeType) AS ?frequency)
WHERE {
  ?workRole a nice:WorkRole ;
           posthuman:posthumanAnalysis ?analysis .

  ?analysis posthuman:primaryCategories ?category .
  ?category a ?codeType .

  FILTER(?codeType IN (
    posthuman:HTE-S,
    posthuman:SE-C,
    posthuman:NHA-S,
    posthuman:SE-I,
    posthuman:AL-T

posthuman:PP-I
    posthuman:PP-E
  ))
}
GROUP BY ?codeType
ORDER BY DESC(?frequency)
```

Query 2 Results

Aggregated frequencies from OG-015 validated analysis and representative work roles

Code Type	Frequency	Description
posthuman:SE-C	64	Socio-Ecological Awareness - Complexity: Recognition of cybersecurity as complex adaptive system
posthuman:HTE-S	49	Human-Technology Entanglement - Symbiosis: Collaborative human-AI relationships maintaining distinct roles
posthuman:NHA-S	23	Non-Human Agency - System Agency: Recognition of autonomous technological decision-making
posthuman:SE-I	18	Socio-Ecological Awareness - Interconnectedness: Understanding of networked dependencies
posthuman:AL-T	12	Adaptive Learning - Technological: Systems that adapt and evolve independently
posthuman:PP-I	8	Posthuman Potential - Integration: Recognition of opportunities for deeper human-technology collaboration
posthuman:PP-E	7	Posthuman Potential - Ethics: Ethical considerations in posthuman contexts

APPENDIX C: Developmental Progression Analysis

This appendix demonstrates the framework's applicability to K-12 standards through a developmental progression analysis of the CYBER.org Threat Actors (THRT) concept area. The analysis traces human-AI collaboration requirements from Kindergarten through Grade 12, revealing how posthumanist competency demands emerge across developmental stages.

Methodology

Four CYBER.org K-12 Cybersecurity Learning Standards (Cyber Innovation Center & CYBER.ORG, 2021) from the Threat Actors (THRT) subdomain were annotated using the posthumanist coding schema. Each standard was analyzed for:

1. **Cognitive level** (Bloom's taxonomy alignment)
2. **Collaboration requirement** (human-centric vs. human-AI collaboration)
3. **Developmental rationale** (pedagogical justification for classification)

Results: THRT Developmental Progression

The following table summarizes the progression of human-AI collaboration requirements across grade bands:

Grade Band	Standard ID	Cognitive Level	Collaboration Type
K-2	K-2.DC.THRT	Describe	Human-Centric
3-5	3-5.DC.THRT	Recognize	Human-Centric
6-8	6-8.DC.THRT	Describe	HTE-S (Symbiotic)
9-12	9-12.DC.THRT	Analyze	HTE-S (Symbiotic)

Detailed Analysis by Grade Band

K-2: Good and Bad Uses of Digital Devices

Standard: *Describe good and bad uses of digital devices*

Classification: Human-Centric
Rationale: At K-2 level, understanding good/bad uses focuses on foundational human judgment and values. Technology serves as the subject of discussion rather than an analytical partner. Students develop basic ethical reasoning through human-guided instruction and concrete examples.
Developmental Justification: Age-appropriate introduction to digital ethics through human mentorship. AI collaboration is neither pedagogically appropriate nor necessary at this developmental stage.

3-5: Motivations Behind Online Behaviors

Standard: *Recognize the different motivations that influence good and bad online behaviors*

Classification: Human-Centric
Rationale: Recognizing motivations requires developing human empathy and social understanding. At this stage, students build foundational social cognition skills through discussion, role-play, and guided reflection with human instructors.
Developmental Justification: Motivation recognition is fundamentally a human social-cognitive skill. Students learn to understand others' intentions through interpersonal interaction, not algorithmic analysis.

6-8: Types of Threat Actors

Standard: *Describe various types of threat actors*

Classification: HTE-S (Symbiotic Human-Technology Entanglement)
Rationale: Understanding threat actor categories benefits from AI-assisted research and current threat landscape information. Students can use AI to explore real-world examples while human instruction provides ethical framing and critical evaluation skills.
Developmental Justification: First grade band where human-AI collaboration becomes pedagogically appropriate. Students are cognitively ready to begin distinguishing AI capabilities from human analytical strengths.
Instructional Implication: Introduce AI as a research partner for exploring threat actor characteristics. Emphasize human judgment in evaluating source credibility and understanding geopolitical context that AI may lack.

9-12: Threat Actor Motive Analysis

Standard: *Analyze the motives of threat actors*

Classification: HTE-S (Symbiotic Human-Technology Entanglement)
Rationale: Threat motive analysis requires symbiotic collaboration: AI excels at pattern recognition across large threat intelligence datasets, while human analysts provide contextual understanding, ethical judgment, and attribution assessment that AI cannot reliably perform.
Developmental Justification: Analysis-level cognitive demands align with sophisticated human-AI collaboration. Students at this level can critically evaluate AI outputs and understand the epistemological limits of algorithmic threat analysis.
Instructional Implication: Assessment should evaluate student ability to synthesize AI-generated threat intelligence with human contextual analysis. Students should demonstrate understanding of what AI contributes (pattern matching, data correlation) versus what requires human judgment (attribution confidence, geopolitical context, ethical implications).

Key Findings

1. **Developmental Transition Point**: Grade 6-8 marks the first grade band where human-AI collaboration becomes pedagogically appropriate for threat analysis competencies.

2. **50/50 Distribution**: Across the four grade bands, half (K-2, 3-5) remain appropriately human-centric, while half (6-8, 9-12) benefit from structured human-AI collaboration.

3. **Cognitive Alignment**: The transition to human-AI collaboration correlates with increased cognitive demands, from basic description and recognition to analytical synthesis.

4. **Pedagogical Implications**:

    - **Early grades (K-5)**: Focus on human mentorship, ethical reasoning, social cognition
    - **Middle school (6-8)**: Introduce AI as research partner with human critical evaluation
    - **High school (9-12)**: Develop sophisticated human-AI collaborative analysis skills

This developmental progression demonstrates the framework's utility for curriculum coordinators designing age-appropriate learning experiences that prepare students for authentic cybersecurity work roles requiring human-AI collaboration.

Enhancing Cybersecurity Awareness in Business Students through Gamified Learning

Mubashrah Saddiqa
msad@mmmi.sdu.dk
University of Southern Denmark
5230 Odense M, Demark

Marie Louise Haagensen
maha@eadania.dk
Business Academy Dania
8960 Randers, Denmark

Niels Østergaard
nios@eadania.dk
Business Academy Dania
8800 Viborg, Denmark

Abstract

Business students often lack cybersecurity awareness, leaving them vulnerable to social engineering and weak authentication practices. This study presents two gamified cybersecurity modules—Social Engineering and Authentication—designed for non-technical business students. The modules were developed collaboratively across three campuses of Business Academy Dania and hosted on the SmartLearning platform, combining storytelling, hands-on exercises, and the "Go Phishing" card game to support practical, scenario-based learning. The paper describes the design, development, and curricular integration of the modules, showing how they were embedded into existing business programs and adapted to diverse student groups. The modules were evaluated with undergraduate business students in two learning modules: Social Engineering (n = 44) and Authentication (n = 42). Pre- and post-assessment results showed substantial learning gains, with average quiz scores increasing from 41% to 78% for the Social Engineering module and from 45% to 82% for the Authentication module. Paired-sample t-tests confirmed significant improvements with large effect sizes (Cohen's d = 6.03 and d = 6.51). Moreover, qualitative feedback indicated strong student engagement and perceived practical relevance of the gamified learning activities. By providing a structured and transferable pedagogical approach, this study offers a model for enhancing cybersecurity awareness among non-technical learners in higher education.

Keywords: Cybersecurity Education, Gamification, Business Students, Social Engineering, Authentication, Experiential Learning.

Recommended Citation: Saddiqa, M., Haagensen, M., Østergaard, N., (2025). Enhancing Cybersecurity Awareness in Business Students through Gamified Learning. *Cybersecurity Pedagogy and Practice Journal;* v5(n1) pp 104-113. DOI#: https://doi.org/10.62273/WOBZ8483

Enhancing Cybersecurity Awareness in Business Students through Gamified Learning

Mubashrah Saddiqa, Marie Louise Haagensen and Niels Østergaard

1. INTRODUCTION

In today's digital world, cybersecurity is essential across all sectors (Mallick & Nath, 2024; Blažič, 2022). While traditionally associated with IT professionals, cybersecurity awareness is crucial for all employees, including business roles, to protect sensitive data and organizational assets (Furnell, 2021; Abrahams et al., 2024; Crumpler et al., 2022). Business students often lack technical training yet will operate in environments vulnerable to phishing, social engineering, and weak authentication practices (Trumbach et al., 2022; Wiechetek et al., 2022; Bhusal, 2021; Desolda et al., 2021; Tirfe et al., 2022). For example, a marketing manager might unknowingly click on a phishing email disguised as a client message, or a finance officer might fall victim to social engineering tactics that trick them into transferring funds to fraudulent accounts. Despite these risks, business programs often overlook essential cybersecurity topics, leaving students vulnerable to threats that could impact operations, reputation, and profitability. This knowledge gap emphasizes the importance of cybersecurity awareness training specifically designed for business students, ensuring they can recognize, prevent, and respond to digital threats in real-world business settings (AlDaajeh et al., 2022).

This study addresses this gap by presenting the design, development, and curricular integration of gamified cybersecurity modules for non-technical business students. The modules were developed across three campuses of Business Academy Dania and are hosted on the SmartLearning platform. SmartLearning (https://www.smartlearning.dk/) is a national Danish e-learning platform used across eight academies. It provides interactive modules, multimedia content, and assessment tools. The modules developed in this study focus on social engineering and authentication. They combine interactive storytelling, hands-on exercises, and the "Go Phishing" card game for practical, scenario-based learning. The design and activities are grounded in research on gamified learning for cybersecurity concepts (Gwenhure & Rahayu, 2024; Saddiqa et al., 2021; Williams et al., 2024).

The study is part of the Sikkerhed på Spil (Security through Gaming) project, which seeks to enhance cybersecurity education through engaging, hands-on learning (Sikkerhed på Spil, 2023). The study is guided by the following research questions:

RQ1. *How can gamified cybersecurity modules be designed to effectively engage non-technical business students?*

RQ2*. How can these modules be integrated into existing business curricula to enhance cybersecurity awareness?*

This study presents an instructional design and implementation approach for developing gamified cybersecurity modules tailored to non-technical business students. Through multi-campus integration and the use of storytelling, interactive exercises, and gamified activities, the work demonstrates how accessible, scenario-based cybersecurity learning can be embedded into existing curricula and scaled through the SmartLearning platform.
The paper is structured as follows: Section 2 provides background; Section 3 outlines methodology; Sections 4–5 describe development and testing; Section 6 presents results; Section 7 discusses limitations; and Section 8 concludes the paper.

2. BACKGROUND

Cybersecurity is increasingly vital across all sectors due to growing digital threats (Safitra et al., 2023). While IT professionals receive extensive technical training, many business students and professionals lack the knowledge to identify and mitigate risks, leaving organizations vulnerable (Sussman, 2021; Afenyo et al., 2023). Business programs often overlook cybersecurity topics, particularly social engineering and authentication, despite these being common sources of organizational breaches (Trumbach et al., 2022; Wiechetek et al., 2022; Bhusal, 2021; Desolda et al., 2021; Tirfe et al., 2022; Shilair et al., 2023; Triplett, 2023). This gap highlights the need for accessible, engaging training tailored to non-technical learners.

Research shows that gamification can enhance learning and engagement, particularly for complex subjects like cybersecurity (Deterding et al., 2011; Subhash & Cudney, 2018; Alshaikh, 2020; Abu-Amara et al., 2021; Gwenhure & Rahayu, 2024). When combined with experiential and constructivist learning approaches, gamified modules contextualize threats in realistic scenarios, promoting active problem-solving and applied knowledge (Lander, 2014; Zaric et al., 2021; Mouheb et al., 2019; Saddiqa et al., 2023a; Saddiqa et al., 2023b). Storytelling, multimedia content, and interactive exercises further support retention and understanding. However, few studies focus specifically on non-technical business students, creating a gap in both research and practice.

The Sikkerhed på Spil (Security through Gaming) project was developed to address this need by providing interactive, gamified cybersecurity modules for business students (Sikkerhed på Spil, 2023). By integrating storytelling, hands-on exercises, and scenario-based activities, these modules aim to equip students with foundational cybersecurity awareness while remaining accessible to learners without technical backgrounds. This study presents the design, development, and integration of these modules into business curricula, offering a pedagogical model for other institutions.

3. METHODOLOGY

The development of the gamified cybersecurity modules followed a structured process aimed at engaging non-technical business students and integrating seamlessly into existing curricula. Three campuses of Business Academy Dania—Viborg, Skive, and Grenaa—collaborated to ensure relevance across diverse programs, including Multimedia Design, Marketing, and Economics.

Local business representatives were consulted to identify the most pressing cybersecurity challenges, while instructors from the participating programs provided guidance on curricular alignment and practical applicability. This input informed the selection of two modules: Social Engineering, focusing on psychological manipulation tactics such as phishing and pretexting, and Authentication, emphasizing secure password practices, multi-factor authentication, and account protection.

The modules were designed for accessibility and engagement, grounded in constructivist learning theory (Zajda, 2021), and delivered through short, focused segments incorporating interactive storytelling, quizzes, and simulations (Clark & Mayer, 2023; Mayer, 2014). Gamification elements, including point scoring and the "Go Phishing" card game, reinforced active learning and motivation (Deterding et al., 2011; Subhash & Cudney, 2018; Gwenhure & Rahayu, 2024; Zaric et al., 2021), while scenario-based exercises contextualized concepts in realistic business environments (Yang & Wu, 2012; Palioura & Dimoulas, 2022). Optional challenge-based platforms such as TryHackMe provided students with hands-on opportunities to practice cybersecurity in controlled settings (TryHackMe, 2025).

Students piloted the modules in iterative testing cycles, providing feedback on clarity, engagement, and usability, which guided subsequent refinements. Pre- and post-module quizzes were used to assess learning gains, complemented by qualitative feedback from both students and instructors.

Qualitative data from open-ended survey responses and focus group discussions were analyzed using thematic analysis following the framework proposed by (Braun & Clarke, 2006). Two researchers independently reviewed the qualitative responses and conducted initial open coding to identify recurring concepts related to engagement, usability, and perceived learning outcomes. The researchers then compared codes and grouped them into broader themes through iterative discussion and refinement. Themes were included if they appeared in at least 20% of responses or were strongly emphasized during the focus group discussion. To enhance validity, preliminary findings were discussed with five student participants during debrief sessions (member checking) to confirm that the interpretations reflected their experiences. The qualitative themes were subsequently triangulated with quantitative survey results to identify consistent patterns across the findings. Table 1 shows the participants' overview.

Participant	Number	Role in Study
Local Business	10	Identified key cybersecurity challenges
Instructors	3	Advised on curriculum alignment
Students	86	Pilot testing and feedback

Table 1. Participants Overview

The study ran from January 2023 to December 2024, encompassing the development, testing, and revision of the cybersecurity modules. Interviews with local businesses and educators were conducted in early 2023 to identify key cybersecurity challenges. The Social Engineering module was developed and tested in late 2023, and the Authentication module was developed and tested in the second half of 2024. Revisions based on iterative feedback were implemented by December 2024. Data from pre- and post-module assessments, student surveys, and focus groups were analyzed in the first half of 2025 to evaluate learning gains and student engagement.

While this study does not use industry-standard programs such as Cisco Networking Academy or Palo Alto Networks courses, it follows European Union Agency for Cybersecurity (ENISA, 2022) and National Institute of Standards and Technology (NIST, 2021) recommendations for simulation-based and gamified learning. The modules aim to equip non-technical business students with practical cybersecurity skills to act securely and responsibly in professional contexts.

The methodology focuses on replicability and scalability, and demonstrates how gamified, scenario-based cybersecurity education can be designed, integrated, and evaluated for non-technical business students.

4. MODULE DEVELOPMENT

The development of the cybersecurity modules was an iterative and collaborative effort, incorporating input from local businesses, educators, and students. Ten companies from the Viborg region provided insights into real-world cybersecurity challenges, emphasizing the importance of employee training in areas such as phishing, social engineering, and authentication. Educators from the Multimedia Design, Marketing, and Economics programs also contributed, ensuring the modules would be feasible and relevant for non-technical business students.

One business owner said,
"*Employees are the weakest link in our cybersecurity strategy. They are often tricked by phishing emails or phone calls, and we see a growing need for awareness training in this area.*"

Another commented,
"*We invest in technology, but we are realizing that human error is often the biggest vulnerability.*"

Regarding authentication, a business owner emphasized,

"*If employees are reusing passwords or not using MFA, that's a huge risk. We need people who are aware of how to secure their accounts.*"

Educators from the Multimedia Design, Marketing, and Economics programs also contributed, ensuring the modules would be feasible and relevant for non-technical business students.

One instructor stated,
"*Teaching cybersecurity awareness is no longer optional—it's essential. Our students need to understand how social engineering tactics work so they can protect both themselves and the businesses they will work for*."

Module	Key Topics	Optional Activities
Social Eng.	Introduction to social engineering concepts (phishing, baiting, pretexting) Storytelling-based phishing scenarios Interactive quizzes to reinforce learning Ransomware simulation	TryHackMe exercises Teacher-guided discussions or group exercises
Auth.	Password security and multi-factor authentication Biometric and certificate-based methods Gamified password strength game Quizzes and case studies	Use of "Have I Been Pwned?" (Hunt, 2025) Optional teacher-led discussion activities
Go Phishing (Game)	Identification of phishing indicators in emails Collaborative problem-solving in small groups	Printed classroom activity Self-paced /Teacher-guided

Table 2. Key Activities and Optional Components in the Cybersecurity Modules

Based on this feedback, two modules were developed: Social Engineering and Authentication. The development process focused

on creating engaging, interactive content that allows students to understand and apply cybersecurity concepts in practical scenarios.

Both modules are integrated into the SmartLearning platform and designed primarily for self-paced learning. However, optional teacher guides support instructors who wish to facilitate discussions or group exercises, enabling classroom integration when desired.

The modules combine interactive storytelling, hands-on exercises, quizzes, and scenario-based activities to reinforce practical cybersecurity skills. Optional activities encourage deeper engagement and exploration.

A summary of the modules and their key components is presented in Table 2.

a. Social Engineering Module

The Social Engineering module introduces students to the psychological tactics used by cybercriminals to manipulate individuals into revealing confidential information or performing unsafe actions. The module employs storytelling, interactive quizzes, and scenario-based ransomware simulations to provide students with experiential learning opportunities.

As optional activities, students can practice phishing scenarios on the TryHackMe platform and participate in teacher-facilitated discussions if the module is used in a classroom setting.

b. Authentication Module

The Authentication module covers secure password practices, multi-factor and biometric authentication, and case studies of real-world authentication failures. Students engage in hands-on exercises such as password strength games and quizzes that reinforce best practices in cybersecurity.

As optional activities, students may explore additional exercises on TryHackMe, use the "Have I Been Pwned?" (Hunt, 2025) tool to evaluate compromised accounts and participate in teacher-guided discussions when integrated into classroom instruction.

c. Go Phishing Card Game

To complement the Social Engineering module, the Go Phishing card game was developed to provide an interactive, scenario-based learning experience. Students work in small groups to identify phishing indicators in a variety of email scenarios, discussing their reasoning and learning from peers. Points are awarded for correct identifications, and immediate feedback reinforces learning. Teachers can use a facilitation guide with discussion prompts, debriefing questions, and guidance on connecting the game outcomes to workplace cybersecurity risks. This activity enhances engagement, critical thinking, and confidence in identifying phishing attempts in real-world contexts, supporting the experiential and gamified design of the modules.

5. TESTING PROCEDURE

The objective of the study was to evaluate the effectiveness of the gamified cybersecurity modules in increasing awareness and understanding of core cybersecurity concepts among non-technical business students. Understanding these concepts is crucial, as business students often enter professional environments in which phishing, social engineering, and weak authentication practices pose significant risks to organizational security.

In the second half of the study period, in-class testing sessions were conducted across the three campuses of Business Academy Dania (Viborg, Skive, and Grenaa), involving students from the Multimedia Design, Marketing, and Economics programs. Both first- and third-semester students participated, providing insights across various stages of their academic progression. First-semester students initially assessed the Social Engineering module, while third-semester students engaged with the revised Social Engineering module alongside the Authentication module.

Table 3. Overview of Module Testing Table 3. Overview of Module Testing Sessions

Module	Students	Activities	Duration	Campus/Programs
Social Eng.	44	Pre/post assessment, videos, quizzes, interactive exercises, qualitative survey, game testing	3-4 hours	Viborg, Skive, Grenaa/ Multimedia Design, Marketing, Economics
Authentication	42	Pre/post assessment, videos, quizzes, interactive exercises, qualitative survey	3-4 hours	Viborg, Skive, Grenaa/ Multimedia Design, Marketing, Economics

In the second half of the study period, in-class testing sessions were conducted across the three campuses of Business Academy Dania (Viborg, Skive, and Grenaa), involving students from the Multimedia Design, Marketing, and Economics programs. Both first- and third-semester students participated, providing insights across various stages of their academic progression. First-semester students initially assessed the Social Engineering module, while third-semester students engaged with the revised Social Engineering module alongside the Authentication module.

Each in-class session lasted approximately 3–4 hours. Students were first introduced to the project and completed a pre-module assessment, including a brief survey and quiz, to gauge their prior knowledge and familiarity with topics such as phishing, ransomware, and password security. Students then explored the modules independently, engaging with interactive elements including videos, quizzes, storytelling simulations, and the Go Phishing card game. Optional activities, such as TryHackMe exercises and the Have I Been Pwned? tools were available for students seeking additional hands-on practice.

Following the module exploration, students completed a post-module assessment and a qualitative survey. The survey collected open-ended feedback on the modules' strengths, challenges, and suggestions for improvement. In addition, a focus group with five students was conducted to gather more in-depth feedback on usability and content clarity. Two instructors reviewed the modules to provide expert perspectives on pedagogical structure, accessibility, and instructional flow.

Given the exploratory nature of the study and the small sample size, qualitative responses were analyzed using thematic analysis, as described in the methodology section.

Informal member checking during debriefs ensured that the summarized findings accurately reflected the students' experiences. The testing results informed revisions to module content, interactive elements, and instructional design, ensuring that both modules were accessible, engaging, and effective for non-technical learners. Table 3 presents an overview of the activities during the module testing session.

6. RESULTS

Pre- and Post-Module Assessment Results
To evaluate learning gains, students completed pre- and post-module quizzes assessing core cybersecurity concepts.

Social Engineering Module (n = 44):

- 19 students had heard of phishing but were unaware of specific techniques like baiting or spear phishing.
- Most students were aware of ransomware but unfamiliar with its operational mechanisms.
- 40 students reported low confidence in protecting themselves against social engineering attacks.

Authentication Module (n = 42):

- 20 students believed they had strong, unique passwords.
- 18 reported prior use of password managers.
- None had used "Have I Been Pwned?" or the TryHackMe platform before.

Post-module assessment:

- In the Social Engineering module, average quiz scores increased from 41% to 78%.
- In the Authentication module, scores increased from 45% to 82%.
- Paired-sample t-tests confirmed significant gains: Social Engineering:

Theme	Positive Aspects	Challenges	Actions Taken
Engagement	Interactive storytelling, hands-on exercises (TryHackMe, Go Phishing, password game)	Some quizzes and interactive elements are confusing	Introduced guides, shorter video segments (3–5 min), and onboarding tutorials
Practical skills	Real-world scenarios like phishing and ransomware simulations	Platform onboarding difficulties, technical jargon	Added tutorials, simplified language, and included a glossary
Clarity & Structure	Moodle course layout, logical progression	Background colors, long text sections	Content restructuring, visual breaks, clear instructions
Teacher Support	Optional teacher guides for discussion or group activities	Not all teachers are familiar with cybersecurity concepts	Teacher guides revised with step-by-step facilitation tips

Table 4. Summary of Qualitative Feedback and Actions Taken

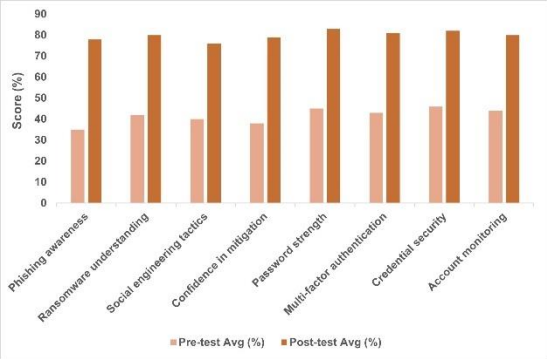


Figure 1. Pre- and Post-Module Quiz Scores for Social Engineering and Authentication Modules

t(43) = 39.99, p < .001, Cohen's d = 6.03; Authentication: t(41) = 42.17, p <.001, Cohen's d = 6.51. These results indicate substantial learning gains between pre- and post-assessments. The large effect sizes reflect the low baseline knowledge observed in pre-assessment, combined with the focused instructional content of the modules.

Student-reported outcomes:

- 40 of 44 students indicated learning practical skills applicable to daily tasks, such as verifying email senders and using stronger passwords
- 39 students enjoyed TryHackMe exercises, noting the real-life scenario experience.
- All students responded positively to the password game for assessing and improving password strength.

Figure 1 shows the overview of pre- and post-module quiz scores for the Social Engineering and Authentication modules.

Qualitative Feedback

Student feedback was collected through surveys, open-ended responses, and focus groups, and was categorized into positive aspects, challenges, and suggestions for improvement. Key results are presented in Table 4.

Student Focus Group Feedback:

- The Moodle platform was user-friendly, but some interactive elements required clearer navigation.
- Students suggested checklists at the end of modules and more localized case studies relevant to Denmark; both were implemented.
- Students also requested additional preventive tips for personal cybersecurity, which were incorporated.

Teacher's Feedback:

- Instructors highlighted the importance of logical flow and accessible language.
- Technical jargon and video transitions need to be improved based on feedback.
- Quizzes need to be clear for intuitive navigation.

Following testing and refinement, both the Social Engineering and Authentication modules were revised based on student and instructor feedback and uploaded to the SmartLearning platform. Instructors across the eight Danish business academies can now provide students with access to self-paced learning, while optional classroom activities, such as discussions, group exercises, or the Go Phishing card game, allow teachers to reinforce practical cybersecurity skills collaboratively. This flexibility accommodates diverse teaching styles and learning contexts, ensuring consistent outcomes across Danish business academies and demonstrating the modules' effectiveness in engaging students and integrating with existing business programs.

7. LIMITATIONS

Despite the findings, the study includes several limitations. First, the study used pre- and post-module assessments but relied on basic inferential statistics (paired t-tests) and descriptive feedback.

Second, the modules were tested in a specific educational and cultural context in Denmark, which may limit transferability to other settings. Finally, although the modules integrate third-party tools like TryHackMe and "Have I Been Pwned?" to provide hands-on learning, these resources are optional based on student interest. Reliance on external platforms may raise concerns about long-term accessibility or technical compatibility, which should be addressed in future scaling.

Despite these limitations, the study contributes valuable insights into designing accessible cybersecurity education for non-technical learners using gamification and experiential methods grounded in proven instructional approaches.

8. CONCLUSION AND FUTURE WORK

This study presented the development and evaluation of two interactive cybersecurity modules designed for non-technical business students. Grounded in experiential and constructivist learning theories, the modules leveraged gamified, scenario-based activities to increase student engagement, understanding, and practical application of cybersecurity concepts. Results demonstrated meaningful learning gains, heightened awareness, and self-reported improvements in security practices.

Instructor and student feedback affirmed the relevance, usability, and motivational aspects of the modules, while also highlighting areas for refinement, such as language simplification, multimedia clarity, and onboarding for optional tools. These insights were incorporated into updated versions. The modules are now accessible to students and instructors across eight Danish business academies via the SmartLearning platform, demonstrating a replicable and scalable approach that could be transferred to other educational contexts.

Future work will focus on developing additional modules and adding more interactive elements. Efforts will also aim to inform teachers about the existence of these modules and provide guidance on how to incorporate them effectively into their teaching, ensuring broader adoption and practical impact.

9. ACKNOWLEDGEMENTS

We thank Andreas Fjord Bonven for his ongoing support, Allan Schnoor for game development and testing, and the eight Danish business academies for their valuable collaboration.

10. REFERENCES

Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M., & Alshehhi, A. (2021). A novel SETA-based gamification framework to raise cybersecurity awareness. International Journal of Information Technology, 13(6), 2371–2380. https://doi.org/10.1007/s41870-021-00760-5

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. Computer Science and IT Research Journal, 5(1), 100–119. https://doi.org/10.51594/csitrj.v5i1.708

Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management, 106493. https://doi.org/10.1016/j.ocecoaman.2023.106493

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies in the improvement of cybersecurity education. Computers & Security, 102754. https://doi.org/10.1016/j.cose.2022.102754

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003

Bhusal, C. S. (2021). Systematic review on social engineering: Hacking by manipulating humans. Journal of Information Security, 12, 104–114. https://doi.org/10.4236/jis.2021.121005

Blažič, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? Education and Information Technologies, 27(3), 3011–3036. https://doi.org/10.1007/s10639-021-10704-y

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

Clark, R. C., & Mayer, R. E. (2023). E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning* (5th ed.). Wiley.

Crumpler, W., & Lewis, J. A. (2022). Cybersecurity workforce gap. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/cybersecurity-workforce-gap

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: A systematic literature review. ACM Computing Surveys, 54(8), 1–35. https://doi.org/10.1145/3469886

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: Defining "gamification." In *Proceedings of the 15th International Academic MindTrek Conference, pp. 9–15. https://doi.org/10.1145/2181037.2181040

European Union Agency for Cybersecurity (ENISA). (2022). ENISA threat landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Furnell, S. (2021). The cybersecurity workforce and skills. Computers & Security, 102080. https://doi.org/10.1016/j.cose.2020.102080

Gwenhure, A. K., & Rahayu, F. S. (2024). Gamification of cybersecurity awareness for non-IT professionals: A systematic literature review. International Journal of Serious Games, 11(1), 83–99. https://doi.org/10.17083/ijsg.v11i1.719

Hunt, T. (2025, Last visited November 16). Have I Been Pwned – Check if your email has been compromised in a data breach. https://haveibeenpwned.com/

Landers, R. N. (2014). Developing a theory of gamified learning: Linking serious games and gamification of learning. Simulation & Gaming, 45(6), 752–768. https://doi.org/10.1177/1046878114563660

Mallick, M. A. I., & Nath, R. (2024). Navigating the cybersecurity landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. World Scientific News, 190(1), 1–69.
https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf

Mayer, R. E. (2014). Incorporating motivation into multimedia learning. Learning and Instruction, 29, 171–173. https://doi.org/10.1016/j.learninstruc.2013.05.001

Mouheb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity curriculum design: A survey. In Transactions on Edutainment XV, 93–107. Springer. https://doi.org/10.1007/978-3-662-59351-6_9

National Institute of Standards and Technology (NIST). (2021). Cybersecurity games: Building tomorrow's workforce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-220.pdf

Palioura, M., & Dimoulas, C. (2022). Digital storytelling in education: A transmedia integration approach for the non-developers. Education Sciences, 12(8), 559. https://doi.org/10.3390/educsci12080559

Saddiqa, M., Larsen, K. H., Nielsen, R. N., & Pedersen, J. M. (2021). Digital innovation in education: Perspectives, opportunities and challenges of educational open data and sensor data. In 2021 Joint Business Informatics Research Workshops and Doctoral Consortium, BIR-WS 2021, CEUR Workshop Proceedings, Vol. 74, 74–83. https://ceur-ws.org/Vol-2991/paper07.pdf

Saddiqa, M., Larsen, K. H., Nielsen, R. N., & Pedersen, J. M. (2023a). Building a diverse cybersecurity workforce: A study on attracting learners with varied educational backgrounds. Journal of Cybersecurity Education, Research & Practice, 2024 (1). https://doi.org/10.32727/8.2023.33

Saddiqa, M., Larsen, K. H., Nielsen, R. N., Sørensen, L. T., & Pedersen, J. M. (2023b). Privacy and security training platform for a diverse audience. In Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Springer Nature Singapore, 343–363. https://doi.org/10.1007/978-981-99-6974-6_19

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369. https://doi.org/10.3390/su151813369

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 102756. https://doi.org/10.1016/j.cose.2022.102756

Sikkerhed på Spil. (2023). Sikkerhed på Spil 2. SmartLearning. Retrieved July 24, 2025, from https://learninghub.smartlearning.dk/projekter/sikkerhed-pa-spil-2/

Subhash, S., & Cudney, E. A. (2018). Gamified learning in higher education: A systematic review of the literature. Computers in Human

Behavior, 87, 192–206. https://doi.org/10.1016/j.chb.2018.01.003

Triplett, W. J. (2023). Addressing cybersecurity challenges in education. International Journal of STEM Education for Sustainability, 3(1), 47–67. https://doi.org/10.52889/ijses.v3i1.132

Tirfe, D., & Anand, V. K. (2022). A survey on trends of two-factor authentication. In Contemporary Issues in Communication, Cloud and Big Data Analytics: Proceedings of CCB 2020, 285–296, Springer. https://doi.org/10.1007/978-981-16-4244-9_23

Trumbach, C. C., Payne, D. M., & Walsh, K. (2023). Cybersecurity in business education: The "how to" in incorporating education into practice. Industry and Higher Education, 37(1), 35–45. https://doi.org/10.1177/09504222221099389

TryHackMe. (Last visited 2025, November 19). TryHackMe – Learn cybersecurity, penetration testing, and ethical hacking. https://tryhackme.com/

Wiechetek, Ł., & Mędrek, M. (2022). Human factors in security–cybersecurity education and awareness of business students. Annales Universitatis Mariae Curie-Skłodowska, Sectio H–Oeconomia, 56(1), 119–142. https://doi.org/10.17951/h.2022.56.1.119-142

Williams, L., Anthi, E., Cherdantseva, Y., & Javed, A. (2024). Leveraging gamification and game-based learning in cybersecurity education: Engaging and inspiring non-cyber students. Journal of The Colloquium for Information Systems Security Education, 11(1), 8.
https://doi.org/10.53735/cisse.v11i1.186

Yang, Y. T. C., & Wu, W. C. I. (2012). Digital storytelling for enhancing student academic achievement, critical thinking, and learning motivation: A year-long experimental study. Computers & Education, 59(2), 339–352. https://doi.org/10.1016/j.compedu.2012.02.003

Zajda, J. (2021). Constructivist learning theory and creating effective learning environments. In Globalisation and Education Reforms: Creating Effective Learning Environments, 35–50. Springer. https://doi.org/10.1007/978-3-030-71575-5_3

Zaric, N., Roepke, R., Lukarov, V., & Schroeder, U. (2021). Gamified learning theory: The moderating role of learners' learning tendencies. International Journal of Serious Games, 8(3), 71–91. https://doi.org/10.17083/ijsg.v8i3.438