Evaluating Cybersecurity Class Activities Based on the Cognitive Continuum Theory: An Exploratory Case Study

Thomas Heverin, Addison Lilholt and Emily Woodward
The Baldwin School, Bryn Mawr, U.S.

thomas.heverin@baldwinschool.org
alilholt@baldwinschool.org
ewoodward@baldwinschool.org

Abstract: With the cybersecurity workforce estimated to have grown to 5.5 million in 2023 but still facing a significant shortage, there is an urgent need for educational strategies that can effectively enhance decision-making skills in this domain. This paper explores the application of Hammond's Cognitive Continuum Theory (CCT) in the context of K-12 cybersecurity education, aiming to address the global cybersecurity workforce shortage and skills gap by preparing the next generation of cybersecurity professionals. This study adopts a case-study methodology to investigate the use of CCT in a high school "Cybersecurity and Ethical Hacking" class, analysing 104 tasks across six class activities to determine how different cognitive modes (Analytical Cognition, Quasi-Rational Cognition, and Intuitive Cognition) are induced by various task characteristics from CCT's Task Continuum Index (TCI). Analytical cognition consists of rational decision making while Intuitive Cognition represents intuitive decision making. Quasi-Rational Cognition represents a blend of these two decision making styles. Directed content analysis and thematic analysis reveal that most tasks in the case promoted Analytical Cognition, with a significant presence of tasks inducing Quasi-Rational Cognition and fewer tasks facilitating Intuitive Cognition. The findings also highlight the dominance of information retrieval and analysis, methodical approaches in information seeking, and synthesis and decision-making across the cognitive modes, pointing towards the critical role of information behaviour in cybersecurity tasks. This research provides insights into how CCT can potentially inform the design of educational activities in cybersecurity, suggesting that a balanced inclusion of tasks across the cognitive spectrum can better prepare students for the complexities of the cybersecurity field. The paper discusses the implications for cybersecurity education, emphasising the need for instructional strategies that encompass a range of cognitive modes to reflect real-world challenges and enhance decision-making capabilities in future professionals. Additionally, the findings make a connection between cybersecurity tasks and school library instruction which focuses heavily on information behaviours. Limitations and directions for future research, including expanding data collection and connecting CCT to other theoretical frameworks, are also discussed.

Keywords: Cybersecurity Education, Cybersecurity Information Seeking, Cognitive Modes

1. Introduction

The ISC2 (2023) cybersecurity workforce annual report, which is based on a global survey, shows a 12.6% annual increase in the workforce shortage, signalling the need for 4 million more cybersecurity professionals. With 67% of respondents noting staff shortages and 92% identifying skills gaps, the urgency for nearly doubling the workforce is evident, especially against the backdrop of the most challenging cybersecurity threat landscape in five years as stated by 75% of respondents (ISC2, 2023).

Addressing this shortfall requires starting cybersecurity education early, at the K-12 level, to boost university enrollments and subsequent workforce readiness, as emphasised by Chen et al. (2021). Cybersecurity tasks vary widely, from simple email analysis to complex malware attack analysis, necessitating a spectrum of decision-making skills—from analytical to intuitive, as described by Heverin (2014) and Hammond (1996). This blend of skills is crucial in high-stakes environments like cybersecurity, where decisions often blend analysis and intuition.

Hammond's Cognitive Continuum Theory (CCT) offers a framework for developing these decision-making skills in K-12 cybersecurity education, balancing analytical and intuitive approaches. However, challenges such as access to technology, age-appropriate content, and effective teaching strategies, along with the time demands of creating engaging class materials, remain significant hurdles (Rowland, Podhradsky, and Plucker, 2018; Chen et al., 2021).

2. Research Background

The CCT, as conceptualised by Hammond (1996), introduces a nuanced perspective in understanding decision-making processes. It delineates three cognitive modes: analytical cognition (AC), intuitive cognition (IC), and quasi-rational cognition (QRC), which is a blend of AC and IC. Rather than dichotomizing IC and AC, CCT places them along a continuum, recognizing the adaptability of human cognition to various task demands.

This continuum is exemplified in the Cognitive Continuum Index (CCI) introduced by Hammond (1996), outlining traits associated with each cognitive mode. The concept of quasi-rationality is central to CCT. This mode is described as "robust and adaptive," fitting for tasks that do not squarely fall into purely intuitive or analytical categories (Dunwoody et al., 2000). The CCI is shown in Table 1.

Table 1: The Cognitive Continuum Theory's Cognitive Modes of Analytical and Intuitive Cognition.

Cognitive Property	Analytical Cognition	Intuitive Cognition
Cue use	Sequential	Simultaneous
Cognitive control	Conscious information processing	Unconscious information processing
Availability of rules	Formal rules available and used	Formal rules unavailable
Cue type	Reliance on quantitative cues	Reliance on qualitative cues
Cue evaluation	Cues evaluated at measurement level	Cues evaluated perceptually
Organising principle	Task specific organising principle	Pattern recognition, averaging

In addition to cognitive modes, CCT connects task characteristics with induced cognitive modes, as seen in the Task Continuum Index (TCI) (Hammond, 1996). The TCI categorises tasks based on properties that evoke IC or AC, thereby offering a comprehensive framework for understanding cognitive mode utilisation in various contexts. The TCI is shown in Table 2.

Table 2: Selected Task Properties from the Task Continuum Index of the Cognitive Continuum Theory.

Task Properties	Analytical Cognition Inducing	Intuitive Cognition Inducing
Number of Cues	Less Than Five	Greater Than Five
Measurement of Cues	Objective	Perceptual
Redundancy Among Cues	Low	High
Decomposition Level of Task	High	Low
Degree of Certainty in Task	High	Low
Display of Cues	Sequential	Simultaneous

The application of CCT across disciplines has been substantial. For instance, in healthcare, studies have explored the relationship between the TCI and the CCI in nurse decision-making, finding correlations between task properties and cognitive modes (Cader, 2005; Conlon, Raeburn, and Want, 2023; O'Connor et al. 2023). This is evidenced in scenarios where nurses, facing high-pressure situations with multiple cues, predominantly engage in intuitive cognition, as observed by Hunter, Consideine, and Manias (2023). Mahan (1994) and Lipshitz (1993) also found support between the correlation of the TCI with the CCI in high-stakes contexts.

Similarly, in cybersecurity, Molinaro and Bolton (2019) revealed that structured tasks, such as tasks phishing email detection, benefit from an analytical cognitive approach. This finding aligns with Heverin's (2019) study, which showed correlations between cybersecurity task properties and cognitive modes in tasks such as phishing email, zero-day exploit analysis, and malware attack detection. The more simple straight-forward tasks (phishing email detection) induced more AC while the more complex tasks (malware attack detection) resulted in inducing more IC (Heverin, 2019).

Moreover, the notion of quasi-rationality in CCT finds a particular resonance in the medical field. Custers (2013) emphasised that clinical problem-solving often occupies the middle ground between pure intuition and analysis. Experienced clinicians, using what Custers refers to as "educated intuition," engage in a more intuitive approach, balancing hypothesis generation with analytical verification.

In a meta-aggregative systematic review of CCT applied to nursing research, O'Connor et al. (2023), found the transferability of CCT to nursing decision making as "high" and that CCT could improve nurse-decision making

and ultimately patient outcomes. Similarly, Cader, Campell, and Watson (2005) used Fawcett's framework, a framework for theory evaluation and testability, to evaluate the CCT and to determine its level of applicability to nurse's decision making. The researchers found empirical evidence across multiple studies that support the concepts and correlations posed by the CCT.

Custers (2013) underscored the importance of exposing novices to a variety of tasks via the TCI, enhancing training by aligning cognitive strategies with task characteristics. This is echoed by O'Connor et al. (2023), who highlighted the significance of incorporating decision-making into education. Cader, Campbell, and Watson (2005) also supported an educational approach based on CCT, arguing it allows for the practice of diverse cognitive modes suited to specific tasks, thereby improving future professional decision-making. Parker-Tomlin et al. (2017) further emphasized CCT training's benefits, particularly for understanding decision-making in team settings and enhancing skills like interprofessional collaboration and communication. Mahan (1994) and Kutschera and Byrd (2005) added that CCT-oriented education fosters superior decision-making strategies over traditional lecture-based methods.

In conclusion, CCT is crucial for understanding decision-making across disciplines, highlighting the CCI and TCI interaction. Integrating CCT into education could enhance future professionals' decision-making abilities, vital for navigating complex environments. Yet, a systematic method to evaluate instructional activities using CCT is missing. Our exploratory study in cybersecurity education begins to address this gap.

3. Methodology

3.1 Case Study Approach

The researchers utilised a case-study methodology for this CCT exploratory study, a strategy that can involve detailed investigation of a single or multiple cases through quantitative, qualitative, or mixed-methods analysis (Yin, 2018). Case studies are valuable for examining phenomena within their natural contexts, with a case typically defined as a phenomenon confined to a specific context and timeframe (Miles, Huberman, and Saldana, 2014). Yin (2018) describes this process as "bounding the case" (p. 31).

In this exploratory case study, the focus was on a high school cybersecurity class of 10 students at a college preparatory school, spanning the September 2023 to January 2024 timeframe. This first of its kind class at the school involved six main cybersecurity activities, including malware analysis and ethical hacking, encompassing a total of 104 tasks. The curriculum aimed at imparting practical skills in cybersecurity tool usage, ethical hacking, network reconnaissance, vulnerability detection, report generation, and malware analysis tasks. Table 3 shows the six main activities and the number of tasks that make up each activity. The results of the ethical hacking tasks were shared with organizations that gave permission for the class to conduct security tests.

Table 3: Malware Activities and Ethical Hacking Activities Analysed for the Case Study.

Malware Activity Cases	Ethical Hacking Activity Cases
Gozi Malware Analysis (14 tasks)	Ricoh Printer Ethical Hacking (11 tasks)
WannaCry Malware Analysis (28 tasks)	Moxa Nport Serial-Ethernet Device Ethical Hacking (13 tasks)
Petya Malware Analysis (28 tasks)	Lantronix Serial-Ethernet Device Ethical Hacking (10 tasks)

The malware tasks focused on using tools such as DynamiteLabs AI and AnyRun which are malware analysis tools freely available in web browsers. The tasks focused on analysing attributes of malware attacks including Gozi, WannaCry and Petya attacks. The ethical hacking tasks focused on using various tools including Shodan, hacking-tools created by the teacher, VirusTotal, Google, ChatGPT and more to conduct ethical hacking of live targets (with permission received ahead of time from the target organisations for testing).

The research questions that guided this exploratory case-study consisted of the following:

- What proportion of malware analysis and ethical hacking tasks in the selected high school cybersecurity class fall into AC, QRC, and IC categories, as determined by predefined TCI criteria?
- Are there differences across the malware analysis and ethical hacking tasks in terms of the AC, QRC, and IC categories?

- What insights can be gained from comparing AC, QRC, and IC tasks identified within malware analysis and ethical hacking tasks beyond the TCI criteria?

To address the first question, the researchers utilised directed content analysis to assess the distribution of cognitive modes tied to specific task characteristics from the TCI. For the second question, they performed inductive thematic analysis on the tasks to identify recurring themes beyond TCI task characteristics. Through these combined analyses, the aim was to thoroughly understand how task characteristics differed across various activities in the cybersecurity learning environment.

3.2 Content Analysis of TCI Task Characteristics

The researchers selected a directed content analysis approach for examining the tasks. Directed content analysis consists of using a deductive approach based on previous theory and uses definitions of coding categories from that theory (Hsieh and Shannon, 2005). In this case, the CCT provided the theoretical framework and the task characteristic coding categories. For this exploratory case study, two researchers conducted the content analysis. Both have several years of computer science and cybersecurity teaching experience at the K-12 and university levels. The lead researcher holds a Ph.D. and research expertise in NDM and CCT as well as several years of operational experience in cybersecurity supporting the U.S. Navy. Given the exploratory nature of this study, two coders were employed to analyse student task data. This approach facilitated the development of a rich initial thematic framework for further investigation in larger studies.

A code book was initially developed based on the TCI. The TCI task characteristics selected were number of cues, measurement of cues, redundancy among cues, decomposition level of task, degree of certainty in task, and display of cues. These are listed above in Table 2 which show which values of the selected TCI characteristics are predicted to induce either AC, QRC or IC.

Two coders independently reviewed a subset of tasks from multiple activities and coded each task as either AC-T, QRC-T, or IC-T, signifying if the task had more AC, QRC, or IC inducing characteristics respectively from the TCI. To ensure consistent application of the coding scheme, two independent coders assessed inter-rater reliability through Cohen's kappa (McHugh, 2012). Initial discrepancies were resolved through discussion, resulting in a final "almost perfect agreement" (kappa = 0.924) for the remaining tasks (McHugh, 2012). Examples of AC-T, QRC-T and IC-T tasks are provided in Table 4.

Table 4: Example tasks falling within each CCT cognitive mode.

Task Characteristics	Example Tasks
AC-T	-Enter the IP address into VirusTotal and state how many vendors marked it as malicious. -For the IP address, state how many ports Shodan shows are open.
QRC-T	-Given that we found open ports on the Nport devices on the target IP address and that you found specific vulnerabilities, state what security recommendations do you have for the university
IC-T	-Before looking at the attack attributes, view the graphical representation only of the malware attack in AnyRun. State what you think may be happening with this attack.

3.3 Thematic Analysis of Tasks within AC-T, QRC-T, and IC-T Categories

After the 104 tasks were coded as falling into AC-T, QRC-T or IC-T categories, the researchers conducted a thematic analysis on the categorised instructions to look for themes beyond measurable task characteristics from the TCI. Thematic analysis aims to uncover and interpret recurring patterns of meaning within qualitative data, providing insights into the underlying themes and experiences it represents (Braun and Clarke, 2006). The researchers followed a traditional six-phase approach to thematic analysis which consists of researchers familiarising themselves with the data, generating initial codes, searching for themes across the data, reviewing and refining those themes, defining and naming them clearly, and finally summarising the findings in a meaningful and comprehensive way (Braun and Clarke, 2006).

4. Results

4.1 Content Analysis Results

Table 5 shows the results of the TCI task characteristics analysis for malware analysis tasks (77), ethical hacking tasks (34) and all tasks combined (104). The table shows that most of the tasks examined in this case study were associated with inducing AC. This means that most of the tasks called for rational and deliberate decision making across malware analysis and ethical hacking tasks. QRC was found to be induced in close to 30% of all tasks. QRC represents a mix of rational and intuitive decision making. To a much lesser extent, IC, which represents intuitive decision making, was found to be induced in 10% or less across malware and ethical hacking tasks.

Table 5: Percentages and counts of tasks that fall within each task type (AC-T, QRC-T or IC-T).

TCI	Percent of Malware Analysis tasks (77 Tasks)	Percent of Ethical Hacking tasks (34 Tasks)	Percent of All Tasks (104 Tasks)
AC-T	66% (46)	65% (22)	65% (68)
QRC-T	24% (17)	32% (11)	27% (28)
IC-T	10% (7)	3% (1)	8% (8)
Total	100% (70)	100% (34)	100% (104)

Various statistical tests were used to examine potential differences in the frequencies of AC-T, QRC-T, and IC-T across the six activities. First, the researchers compared the frequencies of AC-T, QRC-T, and IC-T for two types of tasks (malware analysis and ethical hacking tasks) using a Chi-squared test. While no statistically significant differences were found (chi-square statistic: 2.04, p-value: 0.36), it's important to note that the small sample size may have limited the ability to detect subtle differences. Similarly, a Chi-squared test on frequencies across all six activities together also showed no significant difference (chi-square statistic = 5.12, p-value = 0.88) across AC-T, QRC-T and IC-T.

Given the limitations of sample size, Fisher's exact test for pairwise comparisons was then used. As shown in Table 6, there were significant differences between AC-T and IC-T, as well as QRC-T and IC-T. However, the difference between AC-T and QRC-T was not statistically significant. This aligns with the observed trend of higher frequencies for AC-T compared to QRC-T and IC-T, although further research with larger samples is needed to confirm these findings.

Table 6: Results of Fisher's exact tests for pairwise comparisons for AC-T, QRC-T and IC-T.

Pairwise Comparison	p-value	Interpretation
AC-T vs. QRC-T	0.081	No significant difference
AC-T vs. IC-T	< 0.001	Significant difference: AC-T used significantly more than IC-T
QRC-T vs. IC-T	0.027	Significant difference: QRC-T used significantly more than IC-T

4.2 Thematic Analysis Results

To explore task characteristics beyond the coded categories from the TCI, the researchers performed inductive thematic analysis on each task set (AC-T, QRC-T and IC-T), following Braun and Clarke's approach (2006). This identified recurring themes and patterns within each task set, uncovering insights into task features that influence cognitive engagement beyond task characteristics listed in Table 2. The inductive thematic analysis yielded nine main themes, each containing several sub-themes (20 sub-themes in total). The themes focused on information behaviours which encompass the ways individuals seek, gather, process, apply, and share information. Table 7 summarises the main themes and enumerates the number of sub-themes for each.

Table 7: Identified main themes across the AC-T, QRC-T, and IC-T sets of tasks.

Task Type	Main Themes from Thematic Analysis (Number of Sub-Themes)	Examples
AC-T	Detailed, Precise Information Seeking (4) Detailed Analysis of Information (2) Critical Evaluation of Information (1)	-Find IP addresses in Shodan for a target -Review Shodan results to find open ports -Determine common thread in hostnames
QRC-T	Translation of Information to Advice (4) Adaptive Information Seeking (2) Critical Evaluation of Information Sources (1)	-Recommend mitigations based open ports -Generate searches to identify employee's full name and role based on username -Use multiple sources in and outside of the printer to try to find users of the specific printer
IC-T	Informed Judgement with Uncertainty (3) Active Discovery and Application to New Situations (2) Comparative Analysis and Contrast (1)	-Given 1 malicious link alert, determine risk -Given the map of open industrial control system (ICS) ports in Shodan, state which cities you would defend first and why -Compare and contrast Petya & WannaCry attacks

For AC-T, three main themes emerge: *Detailed Information Seeking for Precise Information*, highlighting detailed searching for precise and accurate information; *Detailed Analysis of Information to Make Decisions,* underscoring detailed analysis of results to make a highly informed decision; and *Critical Evaluation of Information*, focusing on summarising results and assessing the information's accuracy and reliability. This emphasis on a structured and analytical approach facilitates a deep understanding of cybersecurity information, allowing learners to apply this knowledge effectively in practical settings.

QRC-T is characterised by three main themes: *Translation of Complex Information into Advice*, blending technical information results with reasoning to make real-world judgments; *Adaptive Information Seeking*, emphasising iterative strategy refinement and decisions with incomplete information; and *Critical Evaluation of Information Sources,* evaluating which sources provide information and using incomplete information from across sources to make judgements. These themes reflect a dynamic learning environment where students are encouraged to apply technical knowledge adaptively, mirroring the unpredictable nature of cybersecurity challenges.

IC-T's themes include *Informed Judgement in Uncertainty*, fostering decisions based on limited information and scenario-based learning; *Active Discovery and Application*, promoting proactive information search, contextual analysis, and intuitive problem-solving without exhaustive analysis; and *Comparative Analysis and Contrast*, encouraging comparisons and informed assessments. This approach nurtures a proactive and intuitive mindset, preparing students to tackle cybersecurity issues with a blend of critical thinking and adaptability.

Across AC-T, QRC-T, and IC-T tasks, a consistent emphasis on information behaviour underlines the importance of effective information seeking, processing, and application. While AC-T focuses on a detailed and systematic analysis, QRC-T advocates for an adaptive application of technical knowledge in real-world scenarios, and IC-T emphasises intuitive decision-making, based on uncertainty and scarcity of information, and active discovery. These differences highlight the varied information behaviours that appear across the three types of tasks.

5. Discussion

5.1 Research Implications

The case study's finding that cybersecurity tasks predominantly focused on AC, rational decision making, offers a pivotal discussion point. Despite students' engagement with tools like Shodan and Virus Total, the emphasis on AC might have limited the exploration of diverse cognitive modes. This focus could stem from the students' novice status, necessitating structured approaches aligned with AC, or the course's inaugural run prioritising foundational skills. Incorporating more tasks aimed at QRC and IC in future iterations could enrich students' decision-making abilities. Training in varied cognitive modes is suggested to foster "educated intuition" among novices, akin to expert behaviour (Lipshitz and Shual, 1997; Custers, 2013; Mahan, 1994; Cader, Campbell, and Watson, 2005; Kutschera and Byrd, 2005; Parker-Tomlin et al., 2017; O'Connor et al., 2023).

The absence of diverse decision-making strategies in the curriculum calls for attention, though the acquired direct experience with cybersecurity tools is invaluable. Starting with AC might lay the groundwork for later intuitive expertise, reflecting Kolb's Experiential Learning Theory (ELT) where structured learning precedes

intuitive application (Kolb, 1984; Schoonenboom et al., 2008). This approach, suggesting a progression from concrete experience (CE) to active experimentation (AE), mirrors the development from novice to expert. Further research could delve into the parallels between CCT and ELT.

Unexpectedly, the thematic analysis highlighted varied information-seeking behaviours across cognitive modes, underscoring the importance of this aspect in cybersecurity learning. Information behaviour, integral to how individuals seek, process, and utilise information, varied across AC, QRC, and IC tasks, aligning with Taylor's Information Use Environment (IUE) model (1991). The IUE model names 11 problem dimensions (such as "well-structured/ill-structured", "simple/complex", and "susceptible/not susceptible to empirical analysis") that mirror task characteristics found in the CCT's TCI, suggesting a fruitful avenue for future research on the interplay between information behaviours and cognitive modes in cybersecurity learning. According to Taylor, the problem dimensions influence the types of information deemed useful. Taylor (1991, p. 229) stated that problems "pose different requirements on the type of information perceived as necessary, and hence different uses to which information is put in the process of resolution." The potential connection to Taylor's IUE model further implies that the context in which information is sought and used could significantly influence the cognitive modes engaged by learners. For example, using the IUE problem dimensions as a guide, one could develop tasks that are ill-structured, complex, not susceptible to empirical analysis which would most likely induce IC according to the CCT.

5.2 Cybersecurity Education Implications

This study's application of CCT in analysing a high school cybersecurity class presents a unique lens for evaluating educational methods, particularly beneficial for cybersecurity educators. By aligning tasks with the identified TCI task characteristics and information behaviour themes, educators can enhance learning experiences, encouraging students to navigate complex information landscapes through AC, QRC, and IC. Tasks designed to challenge students with evaluating disparate information sources (QRC) or making decisions under data scarcity (IC) are prime examples of how to cultivate essential skills.

The thematic-analysis results in Table 7 show nine high-level themes that focus primarily on information seeking. The high-level themes incorporate 20 sub-themes such as "conduct critical assessments of information gathered", "leverage tools for information gathering," and "synthesize data from disparate sources." These themes align well with the American Association of School Libraries (AASL) Standard Framework for Learners (2018). The AASL Standard contains competencies such as evaluating the quality of information sources, using a variety of tools for information seeking, and comparing information gathered from various sources. Three expert librarians, all who hold a M.S. in Library and Information Science and an average of 12 years of library experience, independently coded the 20 sub-themes in this current study as being related (or not related) to AASL Standard competencies. The results showed a 100% agreement among the librarians for 13 of 20 sub-themes. These initial results show how school library instruction can be embedded in cybersecurity education.

5.3 Limitations and Future Research

This exploratory case study has limitations. The small sample size restricts generalizability. Studying a wider range of cybersecurity tasks and incorporating perspectives beyond just task instructions (teacher reflections, student responses, observations) would provide a more complete picture.

Future research should expand data collection through interviews, surveys, and reflections to enhance credibility and understand how task design influences learning. Sharing lessons would allow for replication studies. Additionally, applying information behavior theories to the framework could offer deeper insights into how tasks influence students' cognitive modes in cybersecurity.

6. Conclusion

This study's exploration into the application of the CCT in K-12 cybersecurity education through a detailed analysis of task characteristics within a high school class reveals a significant tilt towards AC which represents rational decision making. It demonstrates an essential shift is needed towards integrating more IC-inducing tasks (intuitive decision making) and QRC-inducing tasks (a mix of rational and intuitive decision making). This integration aims to balance the range of decision-making strategies used, enhancing students' ability to adapt to the multifaceted challenges of cybersecurity by fostering critical thinking, problem-solving, and adaptive decision-making skills.

Moreover, the study highlights the crucial role of information behaviour in cybersecurity education, aligning with findings to Taylor's IUE model and suggesting pathways for enriching cybersecurity education through the strategic involvement of school librarians. This connection to information behaviour not only aligns with the AASL standards but also opens avenues for interdisciplinary collaboration, emphasising the symbiotic relationship between cybersecurity tasks and librarian instructional practices. Future research is directed towards expanding the CCT framework's application within diverse educational settings, further exploring the interplay between task design, information behaviour, and cognitive modes, and incorporating feedback from students and educators to refine CCT-aligned educational strategies.

Acknowledgements

The authors thank Lauren Friedman-Way and Jessica Tingling of the Baldwin School for providing their librarian expertise.

References

American Association of School Librarians (AASL) (2018) AASL Standards Framework for Learners.

Braun, V. and Clarke, V. (2019) "Thematic Analysis". *Handbook of Research Methods in Health Social Sciences*. Hoboken, New Jersey: Springer. pp. 843–860.

Cader, R., Campbell, S. and Watson, D. (2005) Cognitive Continuum Theory in nursing decision-making. *Journal of Advanced Nursing*, 49(4), pp.397-405.

Chen, W., He, Y., Tian, X. and He, W. (2021) Exploring cybersecurity education at the k-12 level. In *SITE Interactive Conference* (pp. 108-114). Association for the Advancement of Computing in Education (AACE).

Conlon, D., Raeburn, T. and Wand, T. (2023) Cognitive Continuum Theory: Can it contribute to the examination of confidentiality and risk-actuated disclosure decisions of nurses practising in mental health? *Nursing Inquiry*, 30(2), pp. 1-29.

Custers, E.J. (2013) Medical education and cognitive continuum theory: an alternative perspective on medical problem solving and clinical reasoning. *Academic Medicine*, 88(8), pp.1074-1080.

Dunwoody, P.T., Haarbauer, E., Mahan, R.P., Marino, C., and Tang, C. (2000) Cognitive adaptation and its consequences: A test of Cognitive Continuum Theory. *Journal of Behavioral Decision Making*, 13(1), pp.35-54.

Hammond, K.R. (1996) *Human judgment and social policy: Irreducible uncertainty, inevitable error, unavoidable injustice*. New York: Oxford University Press.

Hammond, K. R., Frederick, E., Robillard, N., and Victor, D. (1989) Application of cognitive theory to the student–teacher dialogue. In D. A. Evans and V. L. Patel (Eds.), *Cognitive science in medicine: Biomedical modeling* (pp. 174–210). Cambridge, MA: MIT Press.

Heverin, T. (2014) Information Behaviors and Cognitive Modes Used for Cyber Situation Assessment. Drexel University.

Hsieh, H., and Shannon, S. E. (2005) Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9), pp. 1277–1288.

Hunter, S., Considine, J. and Manias, E. (2023) Nurse decision-making when managing noradrenaline in the intensive care unit: A naturalistic observational study. *Intensive and Critical Care Nursing*, 77.

International Information System Security Certification Consortium (ISC2) (2023) Cybersecurity Workforce Study 2023.

Kolb, D.A. (1984) *Experiential learning: experience as the source of learning and development.* Prentice-Hall, Inc. Englewood Cliffs, NJ.

Kutschera, I. and Byrd, J. (2005) Applying the concept of cognitive continuum to leadership training. *Journal of American Academy of Business*, 6(1), pp.20-25.

Lipshitz, R. (1993) Converging themes in the study of decision making in realistic settings. In Klein, G., Orasanu, J., Calderwood, R., and Zsambok, C. (Eds.), *Decision making in action: Models and methods* (pp.103-137). Westport, CT: Ablex Publishing Corporation.

Lipshitz, R., and Shaul, O. B. (1997) Schemata and mental models in recognition-primed decision making. In *Naturalistic decision making expertise: Research and applications* (pp. 293– 303). Hillsdale, NJ: Erlbaum.

Mahan, R.P. (1994) Stress-induced strategy shifts toward intuitive cognition: A cognitive continuum framework approach. *Human Performance*, 7(2), pp.85-118.

McHugh, M.L. (2012) Interrater reliability: the kappa statistic. Biochem Med (Zagreb), 22(3), pp.276-282.

Miles, M.B., Huberman, A.M., and Saldana, J. (2014) *Qualitative data analysis: A methods sourcebook (3rd ed.)* Thousand Oaks, CA: SAGE.

Molinaro, K.A., and Bolton, M.L. (2019) Using the lens model and cognitive continuum theory to understand the effects of cognition on phishing victimization. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 63(1), pp.173-177.

O'Connor, T., Gibson, J., Lewis, J., Strickland, K. and Paterson, C. (2023) Decision-making in nursing research and practice—Application of the Cognitive Continuum Theory: A meta-aggregative systematic review. *Journal of Clinical Nursing*, 32(23-24), pp.7979-7995.

Parker-Tomlin, M., Boschen, M., Morrissey, S. and Glendon, I. (2017) Cognitive continuum theory in interprofessional healthcare: A critical analysis. *Journal of Interprofessional Care*, 31(4), pp.446-454.

Rowland, P., Podhradsky, A., and Plucker, S. (2018) CybHER: A Method for Empowering, Motivating, Educating and Anchoring Girls to a Cybersecurity Career Path. Paper presented at the *Proceedings of the 51st Hawaii International Conference on System Sciences*.

Schoonenboom, J., Tattersall, C., Miao, Y., Stefanov, K. and Aleksieva-Petrova, A. (2008) The role of competence assessment in the different stages of competence development. *Handbook on Information Technologies for Education and Training*, pp.317-341.

Taylor, R. S. (1991) Information use environments. In Dervin, B. and Voigt, M. J. (Eds.), *Progress in Communication Sciences* (Vol. 10, pp. 217–255). Norwood, NJ: Ablex Publishing Corporation.

Yin, R.K. (2018) *Case study research: Design and methods (6th ed)*. Thousand Oaks, CA: SAGE.