

Play to Protect: Evaluating Cyber Threat Defender in South African Cybersecurity Education

Lance Bunt, Michael De Jager and Luke Coetzee

Unit for Data Science and Computing, North-West University, South Africa

Lance.Bunt@nwu.ac.za

Michael.DeJager@nwu.ac.za

Luke.Coetzee@nwu.ac.za

Abstract: Cybersecurity education in higher education is predominantly theoretical and lecture-centred despite sustained calls for more active and experiential pedagogies. Serious games have been proposed as a promising mechanism for supporting applied reasoning and systems thinking in technical curricula, yet relatively little empirical work examines how students at different stages of disciplinary development perceive such interventions. This study evaluates Cyber Threat Defender (CTD), a strategy-based serious card game designed to simulate cybersecurity concepts such as attack-defence dynamics, risk trade-offs, and layered protection strategies. Using a design-based implementation research approach, CTD was integrated into an undergraduate cybersecurity curriculum at a South African university. The study compares perceptions between two cohorts: second-year students encountering cybersecurity concepts for the first time and final-year students with more developed disciplinary understanding. Quantitative data were collected using Likert-scale instruments measuring perceived educational value, engagement, usability, and curricular relevance, complemented by qualitative responses exploring gameplay experiences and conceptual insights. An additional ruleless second-year session was conducted as a control condition to isolate the influence of instructional clarity on gameplay usability. Descriptive statistical analysis and thematic coding were applied to examine differences in perception across cohorts. Both groups report strong engagement and support for curricular integration of the game, while final-year students demonstrate stronger alignment between gameplay mechanics and cybersecurity concepts. The control condition indicates that rule clarity significantly affects gameplay usability without undermining the perceived educational value of the intervention. The findings further suggest that contextualisation within South African socio-technical environments can enhance the perceived relevance of serious game interventions. These findings suggest that serious games like CTD can support experiential cybersecurity learning when implemented with appropriate instructional scaffolding. The study contributes empirical evidence from a South African context and highlights the role of disciplinary maturity in shaping how students interpret game-based learning interventions.

Keywords: Cross-cohort comparison, Cybersecurity education, Experiential learning, Game-based learning, Higher education, Observational study, Serious games

1. Introduction and Theoretical Background

Cybersecurity education requires students to reason about threats, vulnerabilities, and controls within dynamic socio-technical systems, yet lecture-centred teaching provides limited opportunities to practise these decisions (Hamman & Hopkinson, 2016; Zoto et al., 2019; Lazarov et al., 2025). Serious games may address this limitation by allowing students to test strategies, experience consequences, and discuss competing responses within a safe learning environment. Evidence on how students at different stages of disciplinary development interpret the same serious game intervention remains limited, however. This study addresses that gap by comparing perceptions of the serious game Cyber Threat Defender (CTD) among second-year and final-year cybersecurity students at a South African university.

Specifically, the study aims to evaluate how students at different stages of disciplinary development perceive the educational value, engagement, usability, and curricular relevance of CTD, and to examine how the level of rule guidance relates to its usability within classroom implementation. Four research questions guide the inquiry. RQ1: How do second-year and final-year students differ in their perceptions surrounding the educational value of CTD? RQ2: How do the cohorts differ in perceived engagement and relevance of CTD to cybersecurity learning? RQ3: What qualitative insights emerge regarding the game's role in conceptual understanding of cybersecurity? RQ4: What does the control condition reveal about the role of rule clarity in classroom implementation of serious games like CTD?

Teaching threat modelling and abstract attacker reasoning is difficult in lecture-led formats because students must map symbolic representations (e.g., attacker goals, vulnerabilities, and controls) onto dynamic system behaviour and then apply that reasoning to novel cases under uncertainty (Schiele & Gadyatskaya, 2025). Experiential learning theory (Kolb, 2017) contends that robust understanding develops through iterative movement between concrete experience, reflection, conceptualisation, and active testing, rather than through passive exposure. Cybersecurity education studies reiterate the practical implication: the threat landscape and

the material's intrinsic complexity create limits for traditional educational structures, and undergraduate learners report better engagement and comprehension when teaching includes guided active tasks that surface reasoning through writing and discussion (Srivatanakul & Annansingh, 2022).

Serious games and related game-based approaches support cybersecurity learning by providing safe simulation spaces where learners can rehearse decisions, experience consequences, and iterate strategies without real-world harm, aligning with the field's inherently hands-on nature (Weeratunge et al., 2026). A recent scoping review of 230 primary studies reports wide use of game elements (e.g., time pressure, points, and team-based challenges) and argues for more standardised, mixed-method evaluation designs, combining control comparisons with surveys and interviews, to substantiate learning and transfer claims (Weeratunge et al., 2026). Empirical undergraduate designs also emphasise collaborative reasoning: a cybersecurity escape room study frames undergraduate teaching challenges in terms of complexity and the need for hands-on experience, positioning escape-room mechanics to reinforce course concepts while fostering teamwork and collaboration (Srivatanakul, 2024). Evidence across the literature indicates a persistent design tension: increasing realism can enhance perceived authenticity but does not necessarily guarantee learner transfer, so design choices should prioritise decision-relevant cues and structured reflection that make underlying principles explicit (Kuipers et al., 2017).

The rationale for comparing second-year and final-year cohorts is that educational artefacts are interpreted through learners' existing conceptual frameworks: as domain knowledge grows, mental models typically become more coherent and richly connected, enabling quicker sense-making and more defensible decisions (National Research Council, 2000). In cybersecurity specifically, Zielinska et al. (2015) show that experts' phishing mental-model networks contain more concept linkages than novices', a measurable difference consistent with maturity effects in reasoning and judgment. From a computing education perspective, systematic review evidence indicates that mental models guide task performance and shape how learners understand tasks and representations, implying that more advanced students may extract higher-order principles from the same game or simulation while junior students may focus on surface actions and immediate cues (Heinonen et al., 2023). Cohort comparisons therefore test how disciplinary framing and conceptual maturity moderate perceived usefulness, usability, and learning value, rather than simply comparing preference (Heinonen et al., 2023).

2. Methodology

This section outlines the research design, the CTD game and its mechanics, the participant cohorts and classroom implementation, and the data collection and analytical approach underpinning the study.

2.1 Research Design and Context

This study adopts a quantitative-dominant, observational research design with complementary qualitative insights, conducted within the cybersecurity curriculum at a single South African higher education institution. A cross-cohort comparison was made between second-year and final-year BSc IT students to examine differences in perceived educational value, engagement, usability, and curricular adoption of CTD as a classroom-based learning intervention delivered within scheduled contact sessions. A control dataset from an additional second-year cohort, exposed to a ruleless version of the game, was included selectively to contextualise findings related to rule clarity and usability. The design does not aim to establish causality but rather to identify patterns of association across cohorts under authentic classroom conditions; this framing is consistent with a design-based implementation research approach, in which an educational intervention is evaluated as it is actually delivered rather than under laboratory control.

2.2 The CTD Card Game

Cyber Threat Defender (CTD) is a competitive, turn-based card game in which players build and defend computer networks while attempting to disrupt an opponent's network. Each player begins with a system asset and an internet service provider connection, and draws an initial hand from a shared deck comprising four card types. Asset cards represent computing resources, such as servers, workstations, and internet-connected devices, and generate victory points when successfully added to a player's network. Defence cards are attached to assets to protect them against specific categories of attack, such as firewalls, patching, or encryption. Attack cards target an opponent's undefended or under-defended assets, reducing their score, disabling assets, or forcing discards. Event cards introduce shared conditions that alter the rules of play for all participants, such as simulated outages or policy changes.

On each turn, players draw cards, expand and defend their network, and may launch an attack if strategically advantageous; play continues over multiple rounds until a scoring threshold or round limit is reached, with the highest-scoring, best-defended network declared the winner. Card text explicitly names real-world security controls and threat categories (e.g., distributed denial-of-service attacks, phishing, firewalls, and encryption), so gameplay requires players to reason about which defences neutralise which attacks. These mechanics make the relationships between assets, vulnerabilities, attacks, and countermeasures visible and consequential during play, which is the central pedagogical mechanism evaluated in this study.

2.3 Participants and Classroom Implementation

Participants comprised 177 BSc IT students across three implementation groups: 32 second-year students in a full-rule playtest, 46 second-year students in a rule-limited comparison condition, and 99 final-year students who had previously completed the module in 2025 and therefore had greater disciplinary experience. Participation was based on class enrolment, with no random assignment; the sample reflects a convenience-based educational population, typical of classroom-based studies, and is appropriate for exploratory and comparative analysis of student perceptions within a real-world instructional setting.

Prior gameplay exposure was moderate and broadly comparable across the second-year and final-year focal cohorts (68.8% and 55.6% respectively reported having previously played an educational or strategy card game), while final-year students reported a stronger baseline of cybersecurity concept knowledge (median self-rating of 3, “Good”, IQR 2.0-3.0) than second-year students (median 2, “Fair”, IQR 2.0-2.0), consistent with their prior completion of the module. Age and gender were also captured but were closely comparable across cohorts and are not considered further, as neither would be expected to influence gameplay perceptions in this context; the full descriptive statistics for all instrument items, including these demographic items, are reported in Appendix A.

Gameplay sessions were facilitated in structured classroom environments, with variation in facilitation, timing, and group composition reflecting natural classroom conditions. Each session lasted approximately 60 minutes. Owing to the limited number of available game packs, students played in groups of four to eight, working as teams around a shared pack; individual rounds lasted approximately 13-20 minutes, with the initial round generally taking longer as students became familiar with the cards, and each group completed an average of two to three rounds during the session.

Students in the full-rule condition, comprising both the second-year playtest and final-year cohorts, viewed a gameplay demonstration video beforehand and received printed handouts containing the official rules, explaining game structure, card functions, turn sequence, and conditions for play. Students in the rule-limited comparison cohort received the game packs without demonstration videos, official rule handouts, or structured rule instruction, and were instructed to work out the rules through interaction with the cards and with one another as play progressed. The comparison therefore concerned the level of rule guidance provided rather than access to the game itself. The research team facilitated all sessions: distributing session materials, administering the post-gameplay questionnaire, and observing gameplay to ensure fidelity to the assigned condition, without introducing additional instructional content beyond the materials described above.

2.4 Data Collection and Analysis

Data were collected using a structured questionnaire administered immediately after gameplay. The instrument captured perceived educational value, engagement, usability and rule clarity, and curricular adoption using Likert-scale items, complemented by open-ended questions eliciting qualitative insights into students' gameplay experiences, understanding of cybersecurity concepts, challenges related to rules, and suggestions for contextualisation. The complete questionnaire instrument and item-level descriptive statistics are provided in Appendix A.

Quantitative data were analysed using descriptive statistics, including construct means, medians, and interquartile ranges, to summarise responses across key constructs and to support cross-cohort comparison, with attention to distributional patterns and central tendencies rather than causal inference. Where appropriate, composite scores were calculated to represent broader constructs. Qualitative data from open-ended responses were analysed using thematic coding: responses were reviewed iteratively to identify recurring patterns, which were grouped into five coherent themes reflecting how students interpreted their gameplay experiences (conceptual mapping, strategic reasoning, rules and gameplay flow, collaboration, and contextualisation). This dual approach enabled triangulation between numerical trends and student-reported experiences, supporting a more comprehensive interpretation of the findings.

3. Results and Discussion

The results are organised around cross-cohort comparisons between second-year and final-year student cohorts, with the control dataset introduced where it informs interpretation of usability and rule clarity.

3.1 Learning Value and Engagement

Both focal cohorts reported positive perceptions of CTD's educational value, with consistent agreement that the game supports understanding of cybersecurity concepts and real-world threats. While responses are broadly similar, final-year students demonstrate a slightly stronger alignment between gameplay mechanics and disciplinary concepts, suggesting that prior knowledge supports deeper interpretation of the learning experience. Table 1 presents the cross-cohort comparison of perceived learning value:

Table 1: Cross-cohort comparison of perceived learning value of CTD, including medians, interquartile ranges, and interpretive insights

Questionnaire Item	2nd-Year	Final-Year	Distribution Insight	Interpretation
Content relevance	5 (4-5)	4 (4-5)	Very high agreement for both cohorts	Strong perceived alignment with curriculum
Understanding threats	4 (4-5)	4 (4-5)	High agreement for both cohorts	Consistent perceived learning benefit
Concept explanation confidence	4 (3.8-5)	4 (3-4)	Slightly tighter spread in final-year students	Final-year students show more consistent interpretation
SA context relevance	4 (3-4)	4 (3-5)	Broader spread in final-year students	Contextual relevance recognised but variable
Repeated play clarity	4 (4-5)	4 (3-5)	Strong agreement for both cohorts	Iteration enhances understanding

Overall perceptions of learning value were high for both focal cohorts. The learning value composite score was 4.25 (SD 0.49; median 4.36, IQR 3.96 to 4.61) for second-year playtest respondents and 4.09 (SD 0.56; median 4.00, IQR 3.64 to 4.57) for final-year respondents. The item-level composite cross-cohort differences were small and not statistically distinct after false discovery rate adjustment. At the item level, both cohorts endorsed the relevance of game content to core cybersecurity concepts and reported that gameplay improved their understanding of real-world threats. The only learning-related item showing a meaningful cross-cohort difference after multiplicity control was the statement that playing multiple times made the concepts clearer, rated more strongly by the second-year playtest cohort (mean 4.44) than by the final-year cohort (mean 4.00).

Engagement levels were also high across both cohorts, with strong agreement on enjoyment, motivation, and peer interaction. While second-year students reported slightly higher engagement, the overall pattern indicates that active participation is sustained regardless of disciplinary maturity, and that the interactive structure of CTD consistently promotes engagement. Table 2 compares engagement and participation across the two focal cohorts:

Table 2: Cross-cohort comparison of engagement and participation measures during CTD gameplay

Questionnaire Item	2nd-Year	Final-Year	Distribution Insight	Interpretation
Enjoyment	5 (4-5)	4 (4-5)	Very high agreement for both cohorts	Engagement is consistently strong
Collaboration focus	5 (4-5)	4 (4-5)	Strong agreement for both cohorts	Social mechanics drive engagement
Motivation	5 (4-5)	4 (4-4)	Strong agreement for both cohorts	Active participation is sustained
Peer discussion	4 (3-5)	4 (3-5)	Wide spread for both cohorts	Engagement varies by individual participation

Engagement ratings were high across cohorts, with an engagement composite of 4.44 (SD 0.51; median 4.50, IQR 4.00 to 4.75) for second-year respondents and 4.11 (SD 0.71; median 4.00, IQR 3.75 to 4.75) for final-year respondents. The composite engagement difference did not remain statistically distinct after multiplicity adjustment (MW $p(\text{FDR}) = 0.0657$), although the direction favoured higher engagement in the playtest cohort. At the item level, second-year players reported higher agreement with “*I found the game enjoyable and engaging*” (mean 4.69) than final-year players (mean 4.09). Items related to motivation and peer discussion were similarly high in both cohorts, with smaller differences between them.

3.2 Curricular Adoption

Both cohorts report strong support for integrating CTD into cybersecurity teaching. High and consistent ratings across recommendation and inclusion items suggest that its perceived value is not dependent on prior expertise, indicating its suitability as both an introductory and reinforcing learning tool. Table 3 reports perceptions of CTD's curricular adoption:

Table 3: Cross-cohort comparison of perceptions regarding curricular adoption and integration of CTD.

Questionnaire Item	2nd-Year	Final-Year	Distribution Insight	Interpretation
Recommend CTD	5 (4-5)	4 (4-5)	Strong endorsement for both cohorts	High acceptance of tool
Include CTD in the curriculum	4 (3.8-5)	5 (4-5)	Very strong final-year support	Final-year students see higher curricular value
Memorability vs lectures	4 (4-5)	4 (3-4)	High agreement for both cohorts	Game enhances retention
Games improve learning	5 (4-5)	5 (4-5)	Near-universal agreement	Strong support for game-based learning

Support for curricular adoption was strong in both cohorts. The curricular adoption composite was 4.34 (SD 0.73; median 4.50, IQR 4.00 to 5.00) for second-years and 4.30 (SD 0.80; median 4.50, IQR 4.00 to 5.00) for final-year students, with no meaningful difference (MW $p(\text{FDR}) = 0.8481$). Among final-year students, the retrospective item “*If CTD had been part of the module when I took it, it would have improved my learning*” was rated highly (mean 4.29, SD 0.87; median 4.50, IQR 4.00 to 5.00), indicating that the intervention was perceived as potentially beneficial even when framed as a prior-curriculum enhancement.

3.3 Rule Clarity and Usability

A ruleless second-year playtest session was used as a control to examine the effect of instructional clarity on gameplay experience. This condition isolates usability factors, particularly rule clarity and ease of learning, without evaluating learning outcomes, and allows us to distinguish between the influence of the game design itself and the conditions of its implementation. Table 4 compares usability and rule clarity across the implementation conditions:

Table 4: Comparison of usability and rule clarity perceptions across cohorts, including control condition insights

Questionnaire Item	2nd-Year	Final-Year	Distribution Insight	Interpretation
Ease of learning	4 (4-5)	3 (3-4)	Lower agreement among final-year students	Final-year students more critical of usability
Rule clarity	4 (4-5)	3 (3-4)	Mixed response among final-year students	Instructional clarity affects experience

The ruleless control condition showed substantially lower usability and rule clarity perceptions than the facilitated playtest cohort. The usability composite was 4.13 (SD 0.80) in the second-year playtest cohort versus 2.71 (SD 0.93) in the control cohort, a mean difference of 1.42 (95% CI: 1.02 to 1.81). The individual items “*The game was easy to learn and play after instructions*” and “*The rules were clear and consistent*” both showed similarly large separations, confirming the sensitivity of usability perceptions to instructional clarity and facilitation. Notably, although usability was markedly lower in the rule-control condition, several learning value

and engagement items remained moderately positive, suggesting that the core game concept retained perceived educational promise even under suboptimal implementation conditions.

3.4 Qualitative Insights

Open-ended responses supported five recurring themes. **Mechanics and concepts:** students most frequently cited the attack and defence interactions and card descriptions as clarifying cybersecurity ideas, often emphasising how specific attacks were countered by specific protections. **Strategy and reasoning:** many responses described planning, prioritisation, and resource trade-offs as central to gameplay, aligning perceived learning with an applied decision-making frame. **Rules and flow:** rule complexity and uncertainty were the most frequently reported challenges, particularly in comments describing disrupted flow, delays, or disagreements; in the playtest cohort's dedicated rule clarity prompt, respondents explicitly linked clear rules to improved strategy, confidence, and peer collaboration. **Collaboration:** final-year students more frequently described peer explanation and group coordination as part of gameplay, suggesting that collaborative reasoning was an important part of the perceived learning process. **Contextualisation:** across cohorts, students suggested including more locally relevant cybersecurity scenarios and examples, ranging from locally recognisable threat narratives to explicit requests for stronger alignment with the local curriculum context.

3.5 Discussion

Figure 1 shows the median Likert scores with interquartile ranges across key CTD constructs for second-year, final-year, and control cohorts. Learning value and curricular adoption remain consistently high across cohorts, while engagement shows minor variation; usability demonstrates the most pronounced divergence, with a substantial decrease in the control condition, indicating the critical role of instructional clarity in serious games implementation.

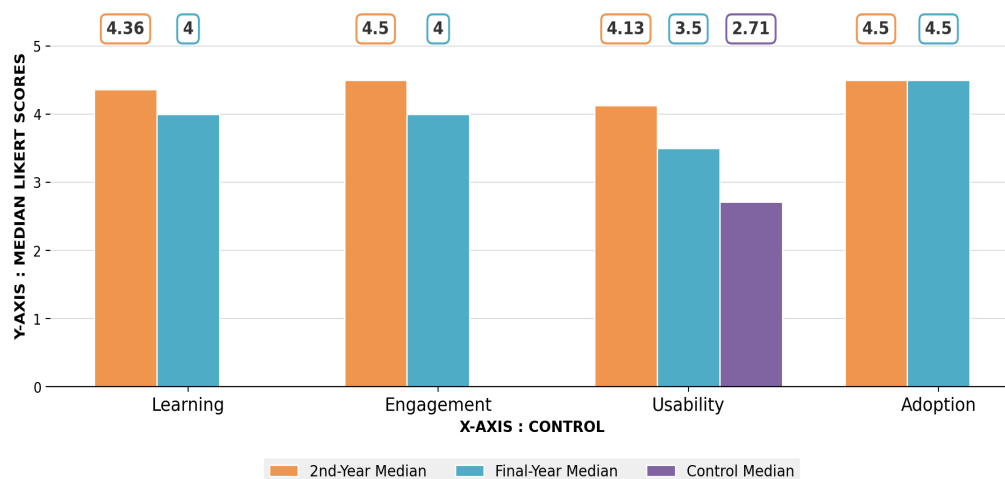


Figure 1: Cross-cohort comparison of median Likert score for CTD constructs (learning, engagement, usability, and adoption)

Disciplinary maturity and perception of learning tools. The cross-cohort comparison showed broadly similar ratings of learning value, suggesting that students at different academic stages can perceive meaningful educational value from a serious game intervention. This aligns with theoretical expectations that experiential learning environments can support knowledge construction through interaction and reflection, even when disciplinary expertise differs. However, final-year respondents were more critical on usability and enjoyment items, and this pattern remained in covariate-adjusted models. A plausible interpretation is that more experienced students hold more stable expectations about instructional efficiency, pacing, or rule formalism, leading to lower tolerance for ambiguity; this is consistent with disciplinary maturity shaping how students interpret the same educational artefact. Engagement was high across cohorts, and item-level results suggested that enjoyment remained a strong component of students' experiences. Serious games are often proposed as pedagogical tools because they combine simulation, decision-making, and interactive feedback loops, which can plausibly support both attention and motivation; the findings here are perception-based, so they do not establish learning gains, but high engagement is relevant for curriculum design because it can increase exposure to conceptual material and promote active discussion, both of which were visible in the qualitative responses.

Implementation design, rule clarity, and curricular integration. The clearest evidence from the dataset concerns implementation: the ruleless control condition produced markedly lower usability and rule clarity ratings, with large effect sizes, directly supporting the claim that facilitation and instructional scaffolding are central to classroom integration of game-based learning interventions. This pattern is robust to analytic choices, appearing in ordinal comparisons, continuous-score sensitivities, and ordinal regression models; proportional-odds sensitivity models, grounded in ordinal regression theory, further suggest substantially lower odds of higher rule clarity ratings in the control condition, reinforcing that rule clarity is not a marginal detail but a primary determinant of the student experience. Students in both focal cohorts supported curricular inclusion, indicating practical viability for CTD as a supplement to conventional teaching and learning approaches such as lecture-based instruction. The strongest actionable implication is that CTD should be deployed with a structured onboarding protocol, such as a short demonstration round, a facilitator script, and a brief rules quiz or checklist, to minimise cognitive load devoted to rule interpretation. The design-based implementation research framing adopted in this study emphasises exactly this kind of alignment between intervention design and implementation conditions.

Contextualisation within a South African setting. While CTD was implemented within a South African higher education context, the quantitative results alone do not strongly distinguish this setting from the broader serious games literature. However, both cohorts indicated moderate agreement that scenarios were appropriate for South African cybersecurity contexts, and qualitative responses consistently called for stronger localisation, including references to locally relevant threats, infrastructure realities, and socio-technical conditions such as mobile-first usage and public-sector vulnerabilities. This suggests that although CTD's core mechanics are broadly transferable, its perceived educational value in this context depends in part on contextual framing; incorporating locally grounded scenarios may enhance relevance by linking abstract concepts to familiar systems, indicating that the game's effectiveness in South Africa is best strengthened through contextual augmentation rather than changes to underlying design.

3.6 Comparisons with Prior Studies and Implications for Cybersecurity Education

The high learning-value ratings are consistent with Srivatanakul and Annansingh (2022), who found that guided activity learning supported engagement and comprehension in undergraduate cybersecurity education; the present findings extend this work by showing comparable perceived value among junior and more experienced students, although prior knowledge appears to shape how explicitly students connect game mechanics to cybersecurity concepts. The qualitative emphasis on peer explanation parallels Srivatanakul's (2024) findings on teamwork and collaboration in cybersecurity escape rooms, suggesting that interaction between students may form part of the learning mechanism rather than serving only as a source of enjoyment.

The reduction in usability under limited rule guidance also supports Weeratunge et al.'s (2026) call, drawn from a scoping review of 230 primary studies, for stronger evaluation of serious game implementation conditions using mixed-method, control-comparison designs; the present study directly answers this call, and its large usability gap between the facilitated and ruleless conditions illustrates why implementation evidence of this kind is needed rather than assumed. The finding that final-year students were more critical of usability, while still recognising the game's underlying educational value, is consistent with Zielinska et al.'s (2015) evidence that more experienced individuals hold more densely connected, higher-order mental models than novices: greater disciplinary maturity appears to sharpen expectations of instructional efficiency and rule formalism as much as it deepens conceptual understanding. This pattern also echoes Kuipers et al.'s (2017) observation that increased realism or complexity in simulation-based learning does not automatically improve transfer, reinforcing the present study's emphasis on structured onboarding and rule scaffolding, rather than increased game complexity, as the more actionable lever for classroom implementation. Taken together, the findings indicate that serious games such as CTD can function as effective complements to traditional cybersecurity instruction by supporting applied reasoning, collaborative learning, and sustained engagement across different stages of disciplinary development. Importantly, the results demonstrate that instructional scaffolding is not optional but central to successful implementation, with rule clarity and structured onboarding directly shaping usability and student experience. The cross-cohort consistency in perceived value further suggests that such interventions can be deployed flexibly, serving both as introductory tools for novices and as reinforcement mechanisms for more advanced learners. These implications highlight the need to treat serious games not only as designed artefacts, but as pedagogical interventions whose effectiveness depends on careful alignment between game design, facilitation, and curricular context.

4. Limitations

Several limitations constrain inference. First, the outcomes are perceptions and self-reports, not objective learning measures. Future work should incorporate pre-post knowledge assessments, performance tasks, or concept-mapping measures to evaluate learning outcomes. Second, this is an observational cross-cohort comparison, so causal attribution is not warranted. Differences between cohorts may reflect facilitation differences, timing, or group composition rather than disciplinary maturity per se; reporting is explicit that the results are associative, consistent with observational reporting standards. Third, Likert items are ordinal. Although the conclusions were robust across ordinal and continuous-score methods, future work could strengthen measurement validity through confirmatory factor analysis, measurement invariance testing across cohorts, and preregistered analysis plans. Fourth, this is a single-institution study with a relatively short gameplay exposure period, limiting generalisability and the extent to which longer-term learning effects can be observed.

5. Conclusion

The study set out to examine how students at different stages of disciplinary development perceive a serious game intervention within a cybersecurity curriculum, and what this reveals about its educational value and implementation. In response to RQ1, both second-year and final-year students reported consistently high perceived educational value, with only minor differences between cohorts. Final-year students, however, demonstrated slightly stronger alignment between gameplay mechanics and underlying cybersecurity concepts, indicating that prior knowledge supports deeper conceptual interpretation. For RQ2, engagement and perceived relevance were high across both cohorts, with second-year students reporting marginally higher enjoyment, while final-year students maintained strong but more moderated responses, suggesting that engagement is sustained irrespective of academic maturity. In relation to RQ3, qualitative findings revealed that students interpret CTD primarily through five dimensions: conceptual mapping of cybersecurity ideas, strategic reasoning and decision-making, the influence of rule clarity on gameplay flow, collaborative interaction, and the need for stronger contextual alignment with real-world and local cybersecurity scenarios. These insights indicate that the game supports applied understanding, not only through its mechanics but through the discussions and reasoning it provokes during play. For RQ4, the control condition provides clear evidence that rule clarity is a critical determinant of usability and overall experience; the absence of structured instruction resulted in substantially lower usability ratings, confirming that facilitation and instructional scaffolding are central to the successful classroom integration of serious games. Importantly, the persistence of moderate learning value perceptions in the control condition suggests that the underlying game design retains educational potential, even when implementation is suboptimal.

Together, these findings indicate that CTD is positively perceived by students across cohorts, that final-year students demonstrate stronger conceptual alignment with the game, and that instructional clarity significantly influences classroom implementation. Serious games such as CTD can therefore serve as valuable tools in cybersecurity education when combined with structured facilitation and deliberate curricular integration.

Ethics Declaration: This study received ethical approval from the North-West University Faculty of Natural and Agricultural Sciences Research Ethics Committee (FNASREC), under ethics number NWU-00594-25-A9. The research was conducted in accordance with institutional ethical guidelines for studies involving human participants. Participation was voluntary and based on normal classroom activities, with no coercion involved. Informed consent was obtained from participants, and no personally identifiable information was collected. All data were anonymised and securely managed to ensure participant confidentiality and data integrity throughout the study.

AI Declaration: Artificial intelligence (AI) tools were used in a limited capacity during the preparation of this paper, primarily to support language refinement, structure, clarity, and editorial improvement. No AI tools were used to generate core research content, data, analysis, or conclusions. All intellectual contributions, including study design, data interpretation, and academic argumentation, remain the original work of the authors. All AI-assisted outputs were critically reviewed and verified by the authors to ensure accuracy, academic integrity, and alignment with scholarly standards. No confidential or sensitive data were shared with AI systems.

References

Cruz-Cunha, M.M. (Ed.), 2012. Handbook of Research on Serious Games as Educational, Business and Research Tools (2 vols). Hershey, PA: IGI Global. <https://doi.org/10.4018/978-1-4666-0149-9>

- Hamman, S.T. and Hopkinson, K.M., 2016. Teaching adversarial thinking for cybersecurity. *Journal of The Colloquium for Information Systems Security Education*, 4(1), p.19.
- Heinonen, A., Lehtelä, B., Hellas, A. and Fagerholm, F., 2023. Synthesizing research on programmers' mental models of programs, tasks and concepts – A systematic literature review. *Information and Software Technology*, 164, p.107300.
- Joshi, S.S., Mukherjee, P., Davis, K.A. and Davis, J.C., 2024. Introducing systems thinking as a framework for teaching and assessing threat modeling competency. *arXiv:2404.16632 [cs.CR]*.
- Kolb, D.A., 2017. *Experiential learning theory as a guide for experiential educators in higher education*. *Experiential Learning & Teaching in Higher Education*, 1(1), pp.7-44.
- Kuipers, D.A., Terlouw, G., Wartena, B.O., van't Veer, J.T., Prins, J.T. and Pierie, J.P.E., 2017. The role of transfer in designing games and simulations for health: systematic review. *JMIR Serious Games*, 5(4), p.e7880.
- Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., Gallus, P. and Fajdiak, R., 2025. Lessons learned from using cyber range to teach cybersecurity at different levels of education. *Technology, Knowledge and Learning*, pp.1-36. <https://doi.org/10.1007/s10758-025-09840-y>
- National Research Council, 2000. *How People Learn: Brain, Mind, Experience, and School* (Expanded ed., Vol. 1). Washington, DC: National Academies Press.
- Schiele, N.D. and Gadyatskaya, O., 2025. A limited technical background is sufficient for attack-defense tree acceptability. In *34th USENIX Security Symposium (USENIX Security 25)*, pp.2225-2244.
- Srivatanakul, T., 2024. Designing cybersecurity escape rooms: A gamified approach to undergraduate learning. *Journal of Cybersecurity Education, Research and Practice*, 2024(1).
- Srivatanakul, T. and Annansingh, F., 2022. Incorporating active learning activities to the design and development of an undergraduate software and web security course. *Journal of Computers in Education*, 9(1), pp.25-50.
- Tene, T., Vique López, D.F., Valverde Aguirre, P.E., Cabezas Oviedo, N.I., Vacacela Gomez, C. and Bellucci, S., 2025. A systematic review of serious games as tools for STEM education. *Frontiers in Education*, 10, 1432982. <https://doi.org/10.3389/feduc.2025.1432982>
- Weeratunge, N.H., Hjelmsvold, R. and Katt, B., 2026. A systematic scoping review on game-based cybersecurity awareness education. *International Journal of Information Security*, 25(2), p.71. <https://doi.org/10.1007/s10207-026-01239-9>
- Zielinska, O., Welk, A., Mayhorn, C.B. and Murphy-Hill, E., 2015. Exploring expert and novice mental models of phishing. In *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security (HotSoS '15)*, Urbana, IL, USA, Article 22, pp.1-2. New York: ACM. <https://doi.org/10.1145/2746194.2746216>
- Zoto, E., Kianpour, M., Kowalski, S. and Lopez-Rojas, E., 2019. A socio-technical systems approach to design and support systems thinking in cybersecurity and risk management education. *Complex Systems Informatics and Modeling Quarterly*, (18), pp.65-75.

Appendix A: Questionnaire Instrument and Descriptive Statistics

Questionnaire item	Item type	2nd-year median	2nd-year IQR	2nd-year n	Final-year median	Final-year IQR	Final-year n
Age Group	Ordered demographic	2 (21-23)	1.8 to 2.0	32	2 (21-23)	2.0 to 2.0	99
Gender	Nominal demographic	N/A	-	32	N/A	-	99
Have you previously played any educational or strategy card games?	Nominal yes/no	N/A	-	32	N/A	-	99
Prior knowledge (self-rating)	Ordered self-rating	2 (Fair)	2.0 to 2.0	31	3 (Good)	2.0 to 3.0	99
The game content appeared relevant to core cybersecurity concepts.	5-pt Likert	5 (Strongly Agree)	4.0 to 5.0	32	4 (Agree)	4.0 to 5.0	99
Playing CTD improved my understanding of real-world cybersecurity threats.	5-pt Likert	4 (Agree)	4.0 to 5.0	32	4 (Agree)	4.0 to 5.0	99
I can explain cybersecurity concepts (e.g., phishing, encryption, firewalls) more confidently after playing CTD.	5-pt Likert	4 (Agree)	3.8 to 5.0	32	4 (Agree)	3.0 to 4.0	99

Questionnaire item	Item type	2nd-year median	2nd-year IQR	2nd-year n	Final-year median	Final-year IQR	Final-year n
CTD scenarios were relevant to South African cybersecurity contexts.	5-pt Likert	4 (Agree)	3.0 to 4.0	32	4 (Agree)	3.0 to 5.0	99
Playing CTD multiple times made the concepts clearer.	5-pt Likert	4 (Agree)	4.0 to 5.0	32	4 (Agree)	3.0 to 5.0	99
What part of the game best illustrated cybersecurity concepts for you?	Open-ended	N/A	-	32	N/A	-	99
I found the game enjoyable and engaging.	5-pt Likert	5 (Strongly Agree)	4.0 to 5.0	32	4 (Agree)	4.0 to 5.0	99
The competitive and collaborative aspects increased my focus.	5-pt Likert	5 (Strongly Agree)	4.0 to 5.0	32	4 (Agree)	4.0 to 5.0	99
I was motivated to participate actively during gameplay.	5-pt Likert	5 (Strongly Agree)	4.0 to 5.0	32	4 (Agree)	4.0 to 5.0	99
I discussed or explained cybersecurity ideas to peers while playing.	5-pt Likert	4 (Agree)	3.0 to 5.0	32	4 (Agree)	3.0 to 5.0	99
Describe one moment where you felt most engaged or curious.	Open-ended	N/A	-	32	N/A	-	98
The game was easy to learn and play after instructions.	5-pt Likert	4 (Agree)	4.0 to 5.0	32	3 (Neutral)	3.0 to 4.0	99
The rules were clear and consistent.	5-pt Likert	4 (Agree)	4.0 to 5.0	32	3 (Neutral)	3.0 to 4.0	99
I would recommend CTD for future cybersecurity courses.	5-pt Likert	5 (Strongly Agree)	4.0 to 5.0	32	4 (Agree)	4.0 to 5.0	99
CTD should be part of the CMPG215 curriculum.	5-pt Likert	4 (Agree)	3.8 to 5.0	32	5 (Strongly Agree)	4.0 to 5.0	99
What challenges did you encounter during gameplay?	Open-ended	N/A	-	32	N/A	-	98
CTD made cybersecurity learning more memorable than standard lectures.	5-pt Likert	4 (Agree)	4.0 to 5.0	32	4 (Agree)	3.0 to 5.0	99
Educational games can improve understanding in technical subjects.	5-pt Likert	5 (Strongly Agree)	4.0 to 5.0	32	5 (Strongly Agree)	4.0 to 5.0	99
How could CTD be adapted to include more South African or African cybersecurity content?	Open-ended	N/A	-	31	N/A	-	96