

A Case Study for Combating Student Overuse of Generative Artificial Intelligence in Cybersecurity Educational Activities Using Augmented Reality Capture-the-Flag Development

Shoshana Sugerman
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0002-9058-6828

Sanya Joseph
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0000-0343-809X

Quinn Colognato
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0005-1274-4685

Mary Cotrupi
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0005-3985-012X

Aanya Mehta
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0002-5651-3385

Tanvi Mehta
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0005-2243-0196

Emily Goldman
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0007-3064-106X

Ishneet Kaur
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0007-6157-3549

Victoria Cai
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0009-7290-9081

Gabriel Bezerra
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0002-1690-0073

Adam Kaplan
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0008-9318-2670

Arielle Revis
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0003-1511-8351

Lala Liu
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0009-0074-4011

Samuel Leung
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0009-2677-9490

Elif Kulahlioglu
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0008-3026-3123

Rachel Schneider
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0004-4844-9779

Mikah Schueller
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0008-0752-4145

Quinn Sharp
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0006-6032-8755

James Porvaznik
*Information Technology
& Web Science Program*
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0007-3820-8711

Brian Robert Callahan
*Department of Computer Science
& Software Engineering*
Monmouth University
West Long Branch, NJ, USA
0000-0002-1797-8633

Abstract—Cybersecurity Capture-the-Flag (CTF) tournaments are well-understood to teach skills necessary for success in today's cybersecurity field. However, that does not mean CTFs are without critique. In the age of Generative Artificial Intelligence (AI), particularly for large-scale CTF tournaments, the use of Generative AI may be permitted or even encouraged to match the reality of today's practitioners, who

are using AI systems to protect data, systems, and people. In such a situation, CTF participants must themselves balance the use of Generative AI with its overuse—effectively self-police the draw to offload one's thinking to the machine in pursuit of correct answers and prizes. In this paper, we introduce a case study for combating the overuse of Generative AI in cybersecurity educational activities through

the building of our own CTF using Augmented Reality (AR) technologies. Written by the nineteen undergraduate students who developed the CTF along with our professor who supervised our work, we argue that using the pedagogic lenses of the “see one, do one, teach one” model and peer learning allowed us to reinterpret our efforts on our CTF into a vision of shared labor and shared responsibility. This reframing of our own understanding of our work effectively acted as a counterbalance, keeping us focused on using Generative AI as a tool and not a crutch, leading to improved educational outcomes for us as individuals and the group as a whole. We hope that documenting our experiences inspires others to adopt similar counterbalance techniques where and when appropriate.

Keywords—*augmented reality, capture-the-flag, cybersecurity, pedagogy, “see one, do one, teach one” model, peer learning*

I. INTRODUCTION

Cybersecurity Capture-the-Flag (CTF) tournaments are a fun and engaging method for learning critical skills necessary for excelling in today’s information security career landscape. When well-executed, participants have a rewarding space to try out new knowledge and experiment with knowledge-in-progress, being given a space accommodating of making mistakes in the course of learning. CTFs also provide both immediate and long-term feedback as to the growth of skill development, with points being immediately awarded on successful solutions as well as future challenges being made easier as skills are further refined. It is no wonder that CTFs are well-researched and highly touted in the literature [1, 2, 3].

However, for all the benefits of CTF participation, they are not without criticism, including excessive difficulty for newcomers, a high barrier to entry [4], unwelcoming culture, and some participants being overly competitive [5]. The professionalization of cybersecurity as an industry is effectively intertwined with the development of CTFs as an event, status symbol, and gatekeeper [6].

We have identified a new potential criticism for CTFs, particularly those that are massively distributed across many schools and geographies: the use and potential overuse of Generative Artificial Intelligence (AI) to solve challenges. Recent studies argue overuse of Generative AI may result in memory loss and increased procrastination [7], increased laziness and underdeveloped cognitive skills [8], loss of critical thinking skills [9, 10], and negative cognitive offloading [11, 12].

In this paper, we, nineteen students who were afforded the educational opportunity to develop our own CTF, and our professor, provide a case study for combating student overuse of Generative AI in cybersecurity educational activities using the development of our own Augmented Reality (AR) CTF tournament, called the Rensselaer Cybersecurity Collaboratory CTF, or RC³TF for short. This work, undertaken when we were all undergraduate students, brings our campus to life as an

enterprise network where players must physically navigate to encounter challenges and uncover the story of a university network under attack by malicious actors and save the day.

Using broad definitions and following the literature reviewing the uses of Virtual Reality (VR) and AR in education, we define VR to mean “a digital representation of a three dimensional object and/or environment” [13] and AR to mean a bridge that enhances the connection between meatspace and digital and virtual space [14, 15]. These definitions align with previous work in the literature and match our understanding of our own CTF.

Our pedagogic goals in this project are to improve student preparation to build a resilient cyber culture, provide an important evaluation of the benefits and risks of AI in cybersecurity education, incorporate students of all skill levels from non-cyber students to domain experts, and flip the script on game-based and project-based learning.

We believe the process we followed represents a model for how Generative AI could be used in project-based cybersecurity education. We understand our work through the lenses of the “see one, do one, teach one” model [16] and peer learning [17]. These lenses allow us to demonstrate clear interventions in our own educational process where overreliance on Generative AI would have made our efforts impossible.

We share our work to provide inspiration to our fellow students and to educators to adopt similar practices to realize the benefits of Generative AI in education without suffering the negative repercussions of its overuse. It is our hope that students and educators find our experiences useful and adopt our work where and when appropriate.

II. BACKGROUND

The Rensselaer Cybersecurity Collaboratory (RCC) has long established a research programme that includes space for exploring cybersecurity pedagogy for its own sake, and puts the students themselves at the forefront of such exploration. Previously, we reported on how to leverage the excitement of quantum computing to enroll students from a wide variety of disciplines into quantum cybersecurity and provided two template projects designed to appeal to a wide variety of skill levels [18].

In May 2024, the RCC won a seed grant from Rensselaer Polytechnic Institute (RPI) to develop a CTF for mass appeal. Our original plan was to develop a CTF that incorporated VR technologies to provide a unique spin on the standard CTF format. The project formally got underway in the Fall 2024 semester.

Many of us are CTF players ourselves. As part of our degree program, cybersecurity students participate every semester in the National Cyber League (NCL), a two-tournament United States-based CTF competition [19]. The NCL hosts an individual tournament, which enrolls over 8,000 entrants each semester, and a team tournament, featuring

over 4,000 teams each semester. Over 500 colleges and universities participate each semester in the NCL.

We will be the first to admit that we use Generative AI to help solve challenges in the NCL, in both the individual and group tournaments. In Fall 2024, the NCL declared that participants could freely use Generative AI in the solving of challenges. It was this Fall 2024 season that solidified our thinking about the overuse of Generative AI.

It was tempting for us to offload our thinking to the Generative AI when we were stuck on challenges, hoping that the machine would solve the problem for us; indeed we were oftentimes successful in that endeavor. Upon the conclusion of the NCL, debriefing as a group we realized that it would have been possible for a player to offload all their thinking to the Generative AI and solve enough challenges to earn a challenge coin, placing in the top 500 of the over 8,000 students who participated in the NCL, despite not doing, and therefore not understanding, the work necessary to solve the challenges.

Indeed, exploratory research finds an automated LLM agent framework where players can connect the Generative AI of their choice and effectively solve most CTF challenges [20]. This may add to the temptation to offload thinking.

Around this time, we learned that our grant money did not permit purchasing hardware, so we needed to shift our plans. Inspired by Pokémon Go and its use of AR to bring the magical world of pet monsters to life, we decided to lean into the idea that we could incorporate the interactive AR elements that make Pokémon Go an exciting and engaging game into a CTF.

The RC³TF is by no means the first to incorporate AR technologies; such initiatives extend back at least twenty years. In 2005, the Naval Postgraduate School commissioned the development of CyberCIEGE, a video game designed to teach fundamental concepts in information assurance through the genre of construction and resource management simulation, a popular video game genre at the time [21, 22]. More recent examples include Hack the Room, an AR experience in which players scan a premade virtual space through a mobile phone to uncover challenges [23]. A prototype of the Cyberinfrastructure Security Education for Professionals and Students (CiSE-ProS) VR/AR simulation designed to support undergraduate cybersecurity education found that students were both very excited to engage with the interactivity of the simulation and most were able to remember the lessons taught in the simulation [24]. There has also been a proliferation of for-profit companies using gamification and at least some elements of AR to teach cybersecurity skills in a CTF-style fashion, most notably TryHackMe [25] and HackTheBox [26]; both also provide industry certifications along with their educational simulation software [27, 28].

Our novel contributions to this space are to design an experience that unites the physical world with cybersecurity CTF educational experiences and to demonstrate that indeed students can develop the experience we would like to have. While our primary inspiration has been shown to impart a

statistically significant increase in physical activity [29], and that might be a niche benefit of the RC³TF as well, our primary motivation was to provide a unique and memorable experience, one that can help overcome some of the critiques of the modern CTF, and one that, at least for the nineteen of us who developed the RC³TF, can serve as a model for counteracting the negative overuse of Generative AI in our education.

III. INTRODUCING THE RC³TF

We previously published on how we made the RC³TF, highlighting our own personal self-reflections of our learning through four lenses: deepening cybersecurity knowledge, articulating cybersecurity knowledge, honing supplemental skills, and fun [30]. We will summarize the main aspects of the RC³TF here.

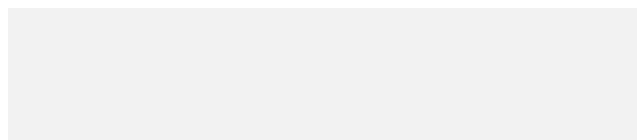
The RC³TF transforms the RPI campus into an enterprise network. We assigned roles to each building, and divided the campus between a Demilitarized Zone (DMZ) and internal network. There is a small bridge that separates our student union building and dorms from the academic buildings on campus; the academic buildings became the internal network and the rest the DMZ, with the bridge itself gaining the role of jump box. Pathways between the buildings were given the role of Ethernet cabling. Players need to physically enter each building to receive challenges germane to that building's role; leaving the building will remove the ability to work on those challenges until players physically return.

Traversing between buildings on the Ethernet cabling may result in random encounters akin to Pokémon Go; these random encounters present famous cybersecurity stories as short vignettes with simple multiple-choice questions at the end to gain additional points and keep players engaged as they walk around campus. As players solve more challenges, a larger story of a campus network under attack begins to unfold, with the players tasked with protecting the network.

Figure 1 shows our finalized game map. Color codings—green for easy, yellow for medium, red for hard—denote difficulty of the challenges found in each building.

When first arriving to the game, players encounter a sign up page and an about page quickly explaining the purpose of the RC³TF. Figure 2 shows the about page and Figure 3 shows the dashboard for players to track their progress.

When players enter buildings, they gain access to that building's challenges so long as they physically remain in the building. For example, when entering the Greene building, one of the internal network PCs, players will be able to access the cryptography challenges. Figure 4 shows the easy cryptography challenge, teaching about the Caesar cipher.



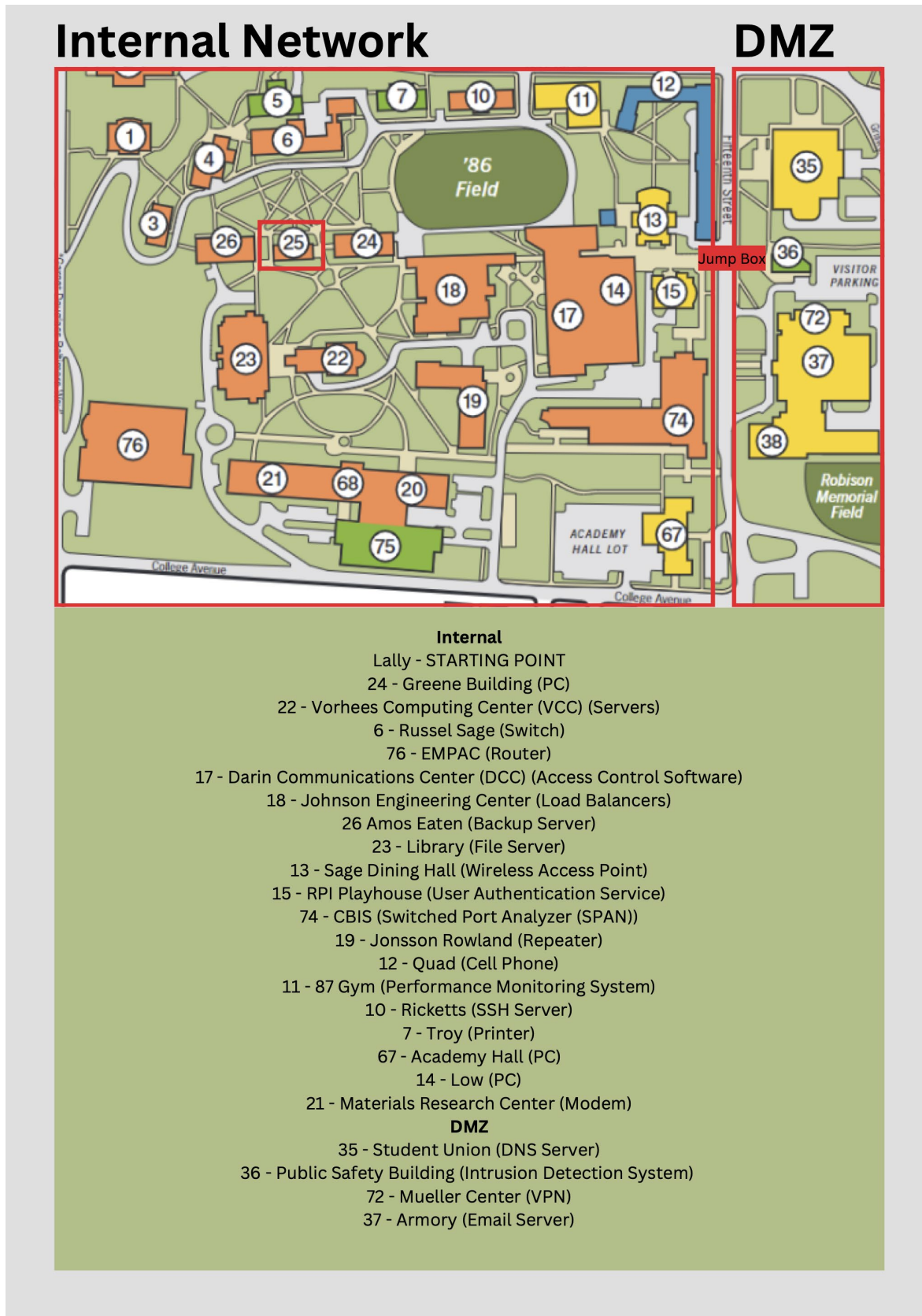


Fig. 1. RC³TF game map transforming RPI campus buildings into an enterprise network.

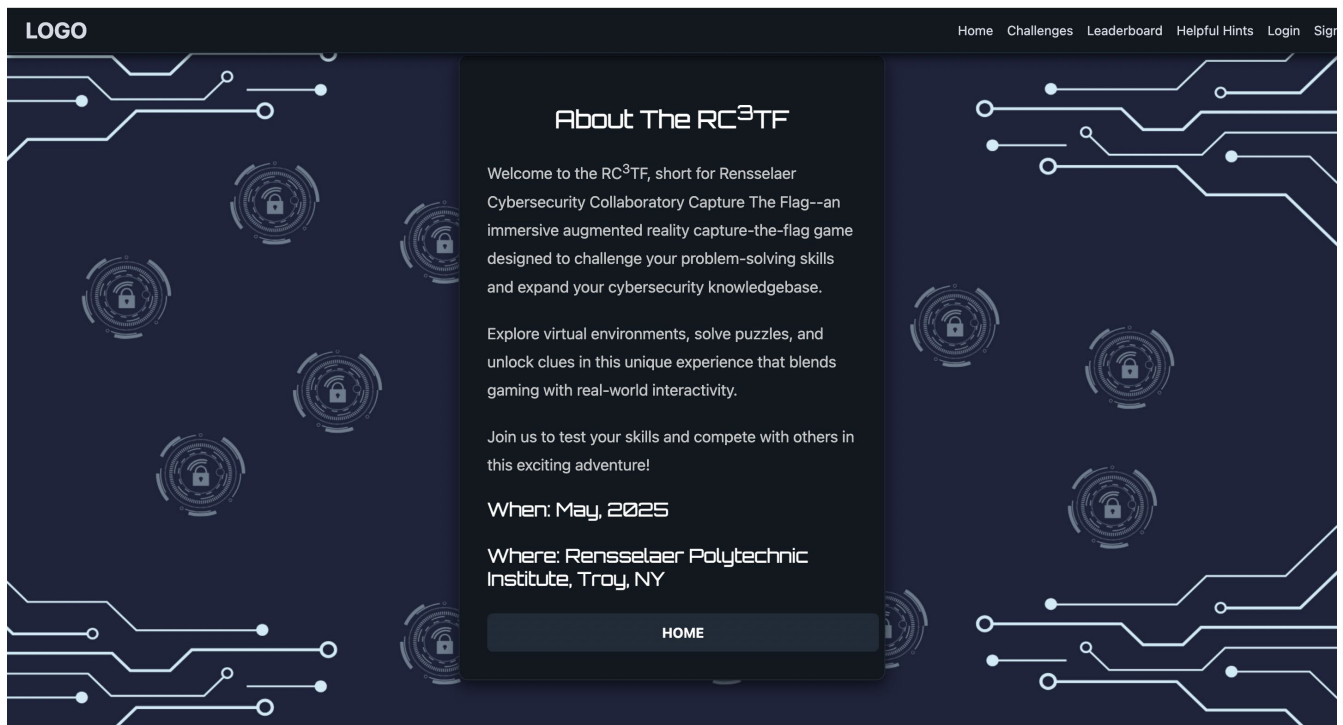


Fig. 2. Image of the About the RC³TF page.

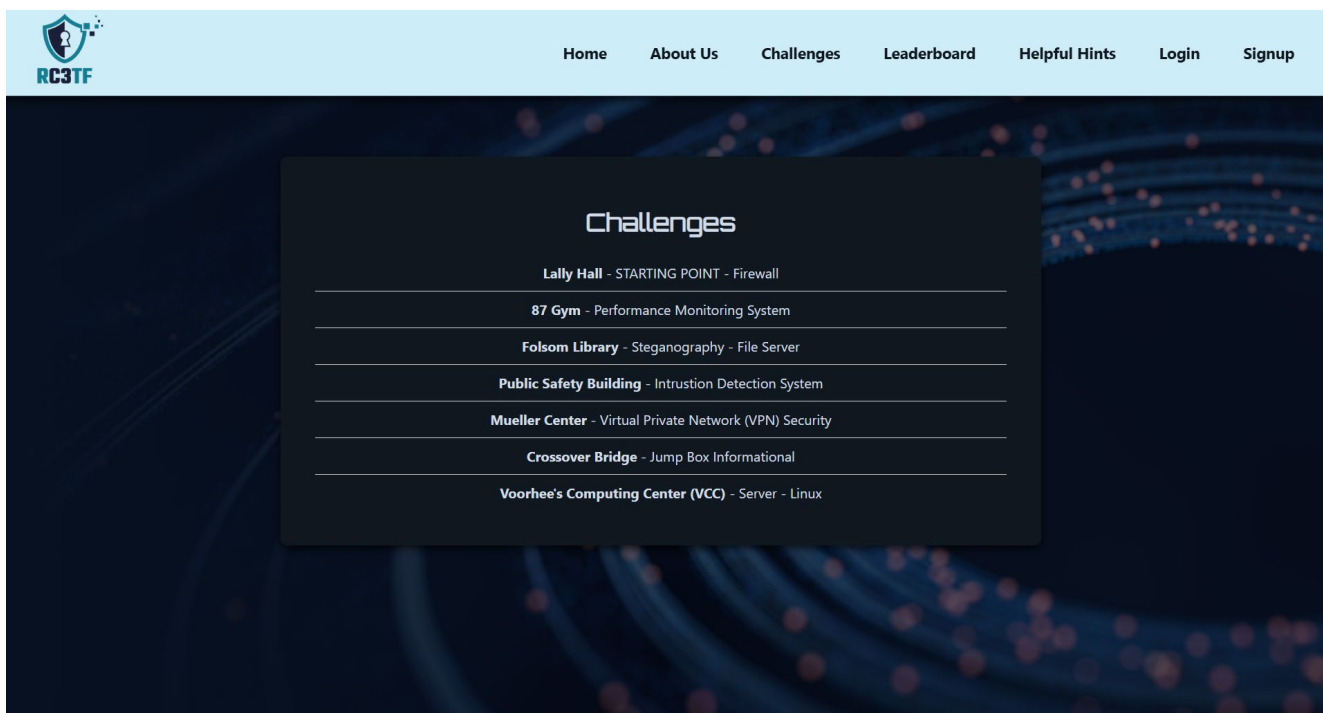


Fig. 3. Image of the player progress dashboard.

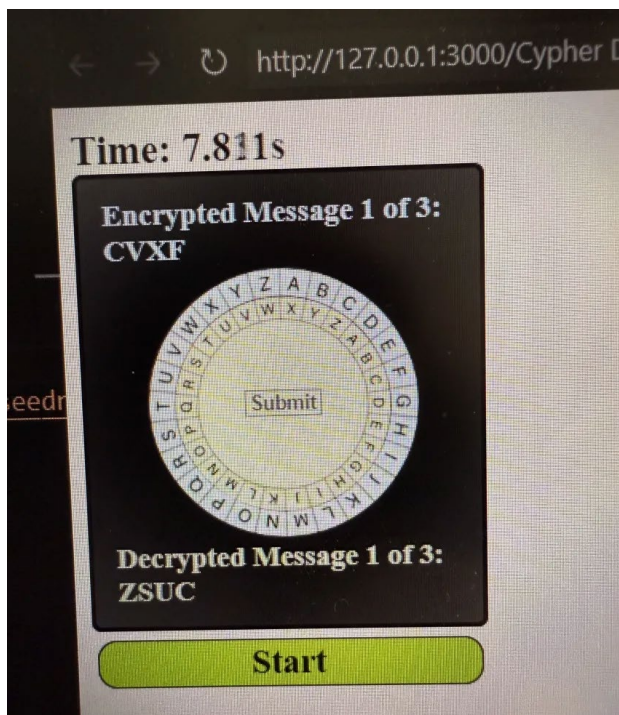


Fig. 4. Image of the Caesar cipher game.

When entering the library, designated the file server, players gain access to file and data related challenges. Figure 5 showcases a game where players need to detect and distinguish corrupted files in a database from clean files.

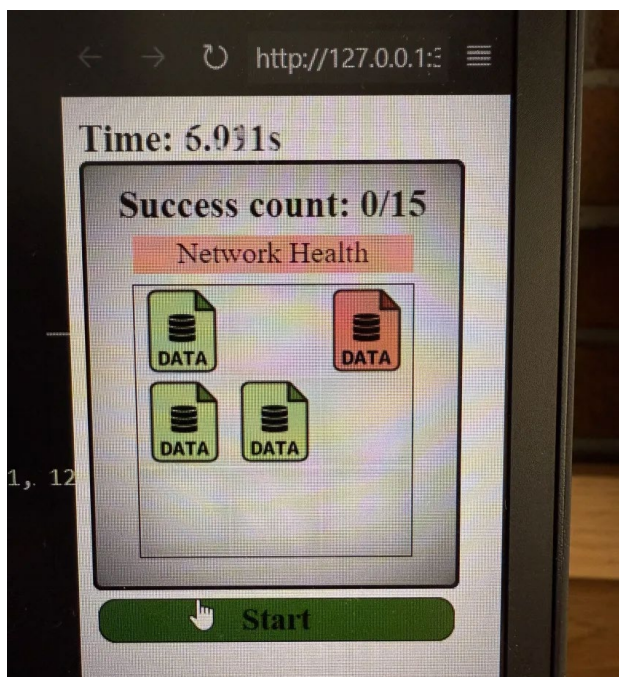


Fig. 5. Image of the Corrupted data detection game.

Traveling between buildings can result in a random encounter. Unlike the challenges inside buildings, which present more like games and traditional CTF challenges, random encounters are designed to be quick, solvable during the short walk between buildings. As such, they present as vignettes with multiple choice or true or false questions to answer. These random encounters serve the dual purpose of keeping players entertained and engaged during what would otherwise be considered “dead time” and teaching about cybersecurity devices and famous cybersecurity events. Figures. 6 and 7 present one such random encounter, teaching about performance monitoring systems.

It is important to mention that the nineteen of us represent a wide variety of expertise, and some of us were total newcomers to cybersecurity when starting this project. For example, the Caesar cipher game was created by a student so new he needed to research what a Caesar cipher even was in order to complete development of the game. On the other hand, the performance monitoring systems vignette was developed by a student who had multiple internships and co-ops in the field. Even so, all of us felt that we were able to meaningfully deepen our cybersecurity knowledge that was appropriate for our personal level, we learned how to better articulate our cybersecurity knowledge particularly for audiences outside the field, and we had fun developing the RC³TF as a group [30].

IV. DISCUSSION

We understand our contributions to counterbalancing the temptation for overuse of Generative AI through two pedagogic lenses: the “see one, do one, teach one” model and peer learning.

A. “See one, do one, teach one”

The “see one, do one, teach one” model originally stems from William Stewart Halsted and his revolutionary training methodology for surgeons at The Johns Hopkins Hospital in Baltimore in the late 19th Century [31]. This model, based on Halsted’s observations of surgeon training in Europe, transformed surgery in the United States from a nearly entirely self-taught discipline to one where students learn from professors, much like today’s system.

The crux of the model is there are three stages in learning any particular skill. First, the student will watch the new-to-them skill be performed. Second, the student will perform the new skill. Third, the student will teach another student, who is at the first stage, the skill [16]. While in surgery this model is no longer acceptable in the modern day due to the very real need to prioritize patient safety, and technology provides simulations so good that surgical students need not perform new skills on live patients [32], the model itself is useful for us in cybersecurity and is likely useful in many other disciplines where skills are not directly performed on humans.

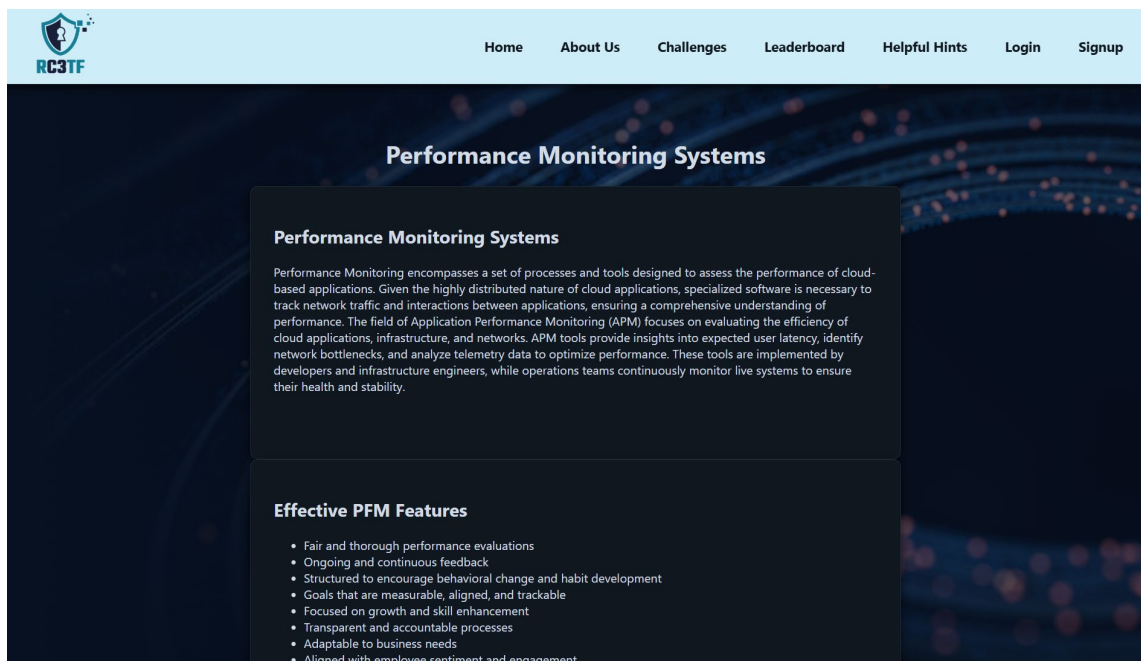


Fig. 6. Random encounter vignette of performance monitoring systems.

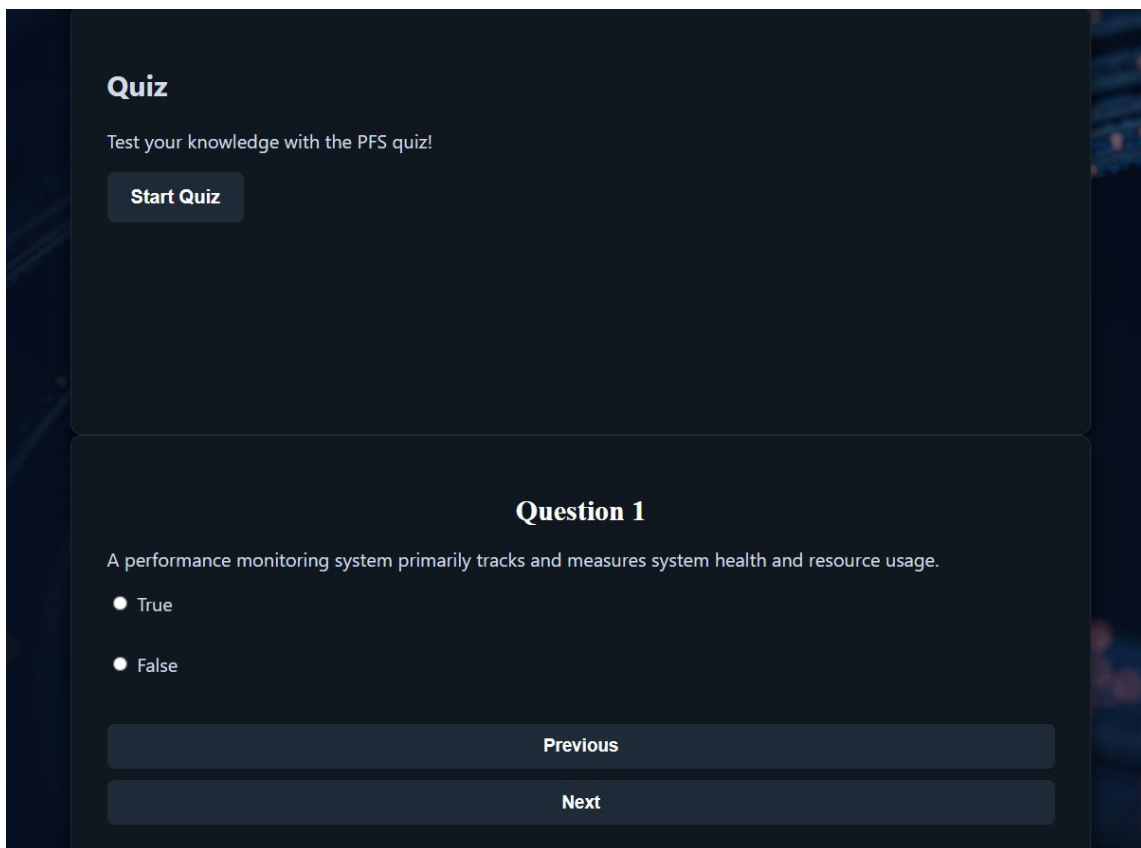


Fig. 7. True or False question at the end of a random encounter vignette.

For many of us, when we first got started playing in the NCL, it would be common for newcomers to be split up among teams primarily composed of more experienced players. In that sense, as newcomers we were able to see all these new cybersecurity skills being used successfully by our teammates and providing us a sense of accomplishment as our teams rose in the ranks. The next semester, we were expected to do a lot more in terms of team contribution, and from that point forward it would be our job to be the ones new players would see, our turn to teach.

That means, even if we did use Generative AI in solving challenges, we were still responsible for teaching the newer students who were watching us. As a result, we actually had to know why our solutions worked. From the informal pressure side, it would not be acceptable to tell newcomers that Generative AI said it was the answer, we got the flag, we can move on now and forget about the challenge; that would only reify criticism in the literature around CTFs having a high barrier to entry [4]. From the formal pressure side, we knew if our professor found out that we were not being good teachers, he would find creative ways to ensure we knew the material and could effectively teach it.

This translated into the RC³TF through our weekly meetings. We met every week as a large group in our professor's office. He expected us to provide meaningful check-ins on our work each week. While we were free to develop the overall game as we saw fit, and we were free to choose which specific challenges we were each going to implement, there was an expectation that at those weekly meetings we would be able to explain what we did—effectively teaching the major concepts to each other.

One example for why this matters: recent work into the effects of Generative AI overuse on cognition showed, among other things, that students were unable to do things like quote from their own work [12]. It would be impossible to teach if we could not even quote from our own work.

While our professor never policed us on how much Generative AI we used in the development of the RC³TF, he would press us if he felt we were not able to adequately explain what we did and the concepts behind it. In that sense, while we could use Generative AI as a tool to help in our individual responsibilities, we could not simply offload all our thinking to the Generative AI, lest we face the consequences of being pressed and potentially embarrassed in front of our peers. We think this informal pressure, though ultimately harmless outside perhaps a temporarily bruised ego, was enough to ensure that we learned the concepts we were responsible for.

B. Peer learning

Peer learning is a pedagogic technique often used in higher education that helps bring a number of “soft skill” benefits to students on top of the direct learning outcomes expected from the content of the learning. These benefits include learning how to collaboratively work with others, how

to take responsibility for one's own learning, and how to deepen one's understanding of the learned content [17]. We follow the definition in Hanson *et al.* 2016 [33] to understand peer learning as a larger umbrella term for pedagogic techniques that includes cooperative learning [34] and collaborative learning [35].

We believe our work falls more in line with the concept of collaborative learning, as cooperative learning emphasizes students working in small groups [34] and we do not believe nineteen students, in essence an entire undergraduate class worth of students, fits with the idea of a small group. However, we do appreciate the idea in cooperative learning that as individuals we only achieve our educational goals when everyone in the group achieves their educational goals [34].

In contrast, collaborative learning affords any number of students greater than one in its definition and specifically calls out the phenomenon of shared labor as learning outcomes are progressed towards [35].

Peer learning provides both educational and psychological benefits to students. Studies show that, using the Ryff scale of psychological well-being [36], peer learning had a statistically significant positive effect on students' feelings of autonomy, environmental mastery, personal growth, purpose in life, and self-acceptance [33].

We lean into the ideas of shared labor and the psychological benefits of peer learning to understand our activities in developing the RC³TF. Generative AI is not, and we believe cannot, be a laborer. As such, it would not be appropriate to completely cognitively offload to the Generative AI; shared labor means equitable shared responsibility. We simply were forced to reconcile with the fact that we respect each other as people, and therefore we are each responsible to ensure that we are all learning and that everyone can benefit from our work. Shared labor means shared respect.

V. CONCLUSION

Nothing in this paper should be understood to mean that we do not advocate for the use of Generative AI in student efforts. We know that Generative AI is fast becoming an expected skill not just in cybersecurity and the Information Technology discipline at large, but an expected skill across a wide array of knowledge work. Research has borne this out, with industry reports suggesting that in 2024, 86% of enterprises are already currently investing in Generative AI or plan to in the next three years [37], a number that has remained steady in 2025 [38].

You can take prompt engineering courses from Microsoft [39] and IBM [40], and be certified in prompt engineering from Vanderbilt University via Coursera [41]. Certification is well-known to establish baselines of knowledge and be a major stage towards professionalization in a wide variety of fields including medicine and librarianship [42], teaching and education [43, 44], and, yes, cybersecurity [27, 28, 45, 46, 47]. This clear move towards professionalization in the Generative

AI space tells us that it is our reality as today's students that our working future fundamentally includes Generative AI, and we would be at a disadvantage if we were to eschew it entirely.

And as we admitted at the beginning of this paper, we too all use Generative AI in our studies. Our critique does not lie with the use of Generative AI but rather the overuse of Generative AI where students offload their thinking fully to the AI, generating correct answers despite not actually learning the underlying material.

It is tempting to suggest that this negative cognitive offloading is solely a detriment to the offending students; the phrase "no one but yourself to blame" (when you fail to learn, fail exams, fail to get a job) comes to mind. Recent studies suggest that Generative AI use comes with excessive negative behavioral and neural consequences [12], and we may be adding fuel to the fire when we carry this "no one but yourself to blame" mindset. Cybersecurity can ill afford to turn away interested practitioners, no matter how skilled or unskilled those practitioners might be today; all can be upskilled.

Industry studies have been sounding the alarm that the cybersecurity industry is suffering a major workforce gap to the tune of nearly five million practitioners globally [48], with understaffing being reported as a major obstacle to properly securing today's organizations [49]. Further industry studies highlight that when hiring entry-level and early-career practitioners, security managers are significantly more likely to prefer hands-on experience and certifications over solely possessing a degree without hands-on experience or certifications [50]. All the more reason that, when we provide students with that hands-on experience, we do our best to ensure they get the most out of those opportunities.

Therefore, we believe it is untrue that only the offending students stand to lose when they offload their cybersecurity education to Generative AI. Cybersecurity is a national security issue for every nation, with recent case studies highlighting Ukraine [51], Canada [52], the European Union [53], and the United States [54], to name just a few. We need all the hands we can get. Moreover, *cybersecurity is a moral issue, and we all stand to lose when anyone fails to learn.*

We can protect learning outcomes in a way that imparts the vital skills learned through CTFs regardless of the amount of Generative AI students use. All it takes is some creative rethinking about how to learn those skills, and putting students in situations where they are called upon to be the experts in their niche and participate in a collegium of student-experts to build skills outside their direct niche. In a real sense, this fulfills Halsted's vision for education.

The pedagogic lenses of "see one, do one, teach one" and peer learning enabled this rethinking. Viewing our work through the "see one, do one, teach one" lens, we participated in CTFs, then worked together as a large group to design the RC³TF, then split off to implement our unique challenges, and finally returned to the large group needing to be able to teach the rest of the group what we learned. Viewing our work

through the peer learning lens, our engagement in shared labor forced us to reconcile with the idea that we were all responsible for each other's success, both in the sense that the RC³TF could not be completed unless we all did our part and in the sense that we were literally responsible for ensuring that everyone in the group learned and understood the concepts we were individually working with. Together, these lenses led us to the understanding that we needed to respect ourselves and each other, which proved enough motivation to reframe our understanding of Generative AI as a tool and not as something to offload our thinking to.

It did not matter how much Generative AI we used; success was defined through our ability to teach each other the material. That is to say, we knew we were successful when we all learned, when we all were able to teach following the "see one, do one, teach one" model, when we all experienced the psychological benefits of peer learning.

We believe our approach to learning cybersecurity skills through the development of our own CTF, led by nineteen undergraduate students, supervised by a professor, and mediated through the lenses of peer learning and "see one, do one, teach one" models is a viable counterbalance to the crutch of the overuse of Generative AI in education. Our efforts improve student preparation to build a resilient cyber culture, provide an important evaluation of the benefits and risks of AI in cybersecurity education, incorporate students of all skill levels from non-cyber students to domain experts, and flip the script on game-based and project-based learning. We believe the model we provide in this paper can scale from small-student groups to massive multi-university events.

We are more excited than ever to run the RC³TF and earn yet another reward for our efforts—the joy of seeing others enjoying the fruits of our labor.

It is our hope that our experiences inspire more students and educators to adopt similar practices in their learning and pedagogy.

ACKNOWLEDGEMENT

We would like to acknowledge the RPI Teaching and Learning Collaboratory, who funded this research with a seed grant. No Generative AI was used in the research or writing of this paper.

REFERENCES

- [1] V. Ford, A. Siraj, A. Haynes and E. Brown, "Capture the Flag Unplugged: an Offline Cyber Competition," *Proc. 2017 ACM SIGCSE Tech. Symp. Comput. Sci. Edu. (SIGCSE '17)*, pp. 225-230, Mar. 8-11, 2017. doi: <https://doi.org/10.1145/3017680.3017783>.
- [2] L. McDaniel, E. Talvi and B. Hay, "Capture the Flag as Cyber Security Introduction," *2016 49th Hawaii International Conf. Syst. Sci. (HICSS)*, Koloa, HI, USA, 2016, pp. 5479-5486, doi: <https://doi.org/10.1109/HICSS.2016.677>.
- [3] S. Kucek and M. Leitner, "An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments," *J. Network and Comput. Appl.*, vol. 151:102470, Feb. 1, 2020. doi: <https://doi.org/10.1016/j.jnca.2019.102470>.

- [4] K. Chung and J. Cohen, "Learning Obstacles in the Capture the Flag Model," *2014 USENIX Summit Gaming, Games, and Gamification Security Edu. (3GSE '14)*, Aug. 18, 2014. [Online]. Available: <https://www.usenix.org/conference/3gse14/summit-program/presentation/chung>.
- [5] J. Warner and P. J. Guo, "Hack.edu: Examining How College Hackathons Are Perceived By Student Attendees and Non-Attendees," *Proc. 2017 ACM Conf. Int. Comput. Edu. Res. (ICER '17)*, pp. 254-262, Aug. 18-20, 2017. doi: <https://doi.org/10.1145/3105726.3106174>.
- [6] N. Fisk, "Developmental Challenges: Capture the Flag and the Professionalization of Cybersecurity," *Hum. Organ.*, vol. 82, no. 1, pp. 61-72, 2023. doi: <https://doi.org/10.17730/1938-3525-82.1.61>.
- [7] M. Abbas, F. A. Jam and T. I. Khan, "Is it harmful or helpful? Examining the causes and consequences of generative AI usage among university students," *Int. J. Edu. Technol. Higher Edu.*, vol. 21, article no. 10, pp. 1-22, 2024. doi: <https://doi.org/10.1186/s41239-024-00444-7>.
- [8] Y. Fan, L. Tang, H. Le, K. Shen, S. Tan, Y. Zhao, Y. Shen, X. Li and D. Gašević, "Beware of metacognitive laziness: Effects of generative artificial intelligence on learning motivation, processes, and performance," *Brit. J. Edu. Technol.*, vol. 56, no. 2, pp. 489-530, Mar. 2025. doi: <https://doi.org/10.1111/bjet.13544>.
- [9] D. Lindebaum and P. Fleming, "ChatGPT Undermines Human Reflexivity, Scientific Responsibility and Responsible Management Research," *Brit. J. Manage.*, vol. 35, no. 2, pp. 566-575, Apr. 2024. doi: <https://doi.org/10.1111/1467-8551.12781>.
- [10] B. Z. Larson, C. Moser, A. Caza, K. Muehlfeld and L. A. Colombo, "Critical Thinking in the Age of Generative AI," *Acad. Manage. Learning & Edu.*, vol. 23, no. 3, pp. 373-378, Aug. 30, 2024. doi: <https://doi.org/10.5465/amle.2024.0338>.
- [11] P. Shukla, P. Bui, S. S. Levy, M. Kowalski, A. Baigelenov and P. Parsons, "De-skilling, Cognitive Offloading, and Misplaced Responsibilities: Potential Ironies of AI-Assisted Design," In *Proc. Extended Abstracts CHI Conf. Human Factors Comput. Syst. (CHI EA '25)*, article no. 171, 1-7, Apr. 26-May 1, 2025. doi: <https://doi.org/10.1145/3706599.3719931>.
- [12] N. Kosmyna, E. Hauptmann, Y. T. Yuan, J. Situ, X-H. Liao, A. V. Beresnitsky, I. Braunstein and P. Maes, "Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task," *arXiv: Comput. Sci.: Artificial Intelli.* doi: <https://doi.org/10.48550/arXiv.2506.08872>.
- [13] S. Kavanagh, A. Luxton-Reilly, B. Wuensche and B. Plimmer, "A systematic review of Virtual Reality in education," *Themes Sci. & Technol.*, vol. 10, no. 2, pp. 85-117, Dec. 27, 2017.
- [14] H-K. Wu, S. W-Y. Lee, H-Y. Chang and J-C. Liang, "Current status, opportunities and challenges of augmented reality in education," *Comput. & Edu.*, vol. 62, pp. 41-47, Mar. 2013. doi: <https://doi.org/10.1016/j.compedu.2012.10.024>.
- [15] K. Lee, "Augmented Reality in Education and Training," *TechTrends*, vol. 56, pp. 13-21, Feb. 7, 2012. doi: <https://doi.org/10.1007/s11528-012-0559-3>.
- [16] S. M. Ayub, "'See one, do one, teach one': Balancing patient care and surgical training in an emergency trauma department," *J. Global Health* 2022; 12:03051, Jul. 6, 2022. doi: <https://doi.org/10.7189/jogh.12.03051>.
- [17] D. Boud, R. Cohen and J. Sampson, "Peer Learning and Assessment," *Assessment & Evaluation Higher Edu.*, vol. 24, no. 4, pp. 413-426, 1999. doi: <https://doi.org/10.1080/0260293990240405>.
- [18] B. R. Callahan, K. Schilp, Q. Colognato, E. Goldman, S. Sugerman, A. Mehta, A. Imanuel, K. Kaii and H. Rose, "Multidisciplinary Quantum Cybersecurity Research for the Undergraduate Laboratory," *J. Colloq. Inform. Syst. Security Edu.*, vol. 12, no. 1, pp. 1-7, Apr. 20, 2025. doi: <https://doi.org/10.53735/cisse.v12i1.206>.
- [19] P. Wang and H. D'Cruze, "The role of cyber competitions in cyber defense education: A case study of the National Cyber League (NCL) participation," *Issues Inform. Syst.*, vol. 23, no. 3, pp. 128-138, 2022. doi: https://doi.org/10.48009/3_iis_2022_111.
- [20] Y. Zou, Y. Hong, J. Xu, L. Liu and W. Fan, "Leveraging Large Language Models for Challenge Solving in Capture-the-Flag," *2024 IEEE 23rd Int. Conf. Trust, Security and Privacy Comput. and Commun. (TrustCom)*, Sanya, China, 2024, pp. 1541-1550, doi: <https://doi.org/10.1109/TrustCom63139.2024.00213>.
- [21] C. E. Irvine, M. F. Thompson and K. Allen, "CyberCIEGE: gaming for information assurance," in *IEEE Security Privacy*, vol. 3, no. 3, pp. 61-64, May-Jun. 2005. doi: <https://doi.org/10.1109/MSP.2005.64>.
- [22] M. Thompson and C. Irvine, "Active learning with the CyberCIEGE video game," *4th Workshop Cyber Security Experimentation and Test (CSET 11)*, Aug. 8, 2011. [Online]. Available: https://www.usenix.org/legacy/events/cset11/tech/final_files/Thompson.pdf.
- [23] M. Korkiakoski, A. Antila, J. Annamaa, S. Sheikhi, P. Alaveses and P. Kostakos, "Hack the Room: Exploring the potential of an augmented reality game for teaching cyber security," In *Proc. Augmented Humans Int. Conf. 2023 (AHs '23)*, pp. 349-353, Mar. 12-14, 2023. doi: <https://doi.org/10.1145/3582700.3583955>.
- [24] J. H. Seo, M. Bruner, A. Payne, N. Gober, D. McMullen and D. K. Chakravorty, "Using Virtual Reality to Enforce Principles of Virtual Reality," *J. Computational Sci. Edu.*, vol. 10, no. 1, pp. 81-87, Jan. 2019. doi: <https://doi.org/10.22369/issn.2153-4136/10/1/13>.
- [25] "Learn Cyber Security | TryHackMe Cyber Training." Accessed: Jun. 12, 2025. [Online]. Available: <https://tryhackme.com/>.
- [26] "Hack The Box: The #1 Cybersecurity Performance Center." Accessed: Jun. 12, 2025. [Online]. Available: <https://www.hackthebox.com/>.
- [27] "TryHackMe | Security Analyst Level 1 (SAL1) Certification." Accessed: Jun. 12, 2025. [Online]. Available: <https://tryhackme.com/certification/security-analyst-level-1>.
- [28] "Cybersecurity Certifications | Prove Practical Skills. Get Hired." Accessed: Jun. 12, 2025. [Online]. Available: <https://academy.hackthebox.com/preview/certifications>.
- [29] M. Khamzina, K. V. Parab, R. An, T. Bullard and D. S. Grigsby-Toussaint, "Impact of Pokémon Go on Physical Activity: A Systematic Review and Meta-Analysis," *Amer. J. Preventative Med.*, vol. 58, no. 2, pp. 270-282, Feb. 2020. doi: <https://doi.org/10.1016/j.amepre.2019.09.005>.
- [30] B. R. Callahan, S. Joseph, S. Sugerman, Q. Colognato, A. Mehta, T. Mehta, E. Goldman, M. Cotrupi, I. Kaur, V. Cai, G. Bezerra, A. Kaplan, A. Revis, L. Liu, S. Leung, E. Kulahlioglu, R. Schneider, M. Schueller, Q. Sharp and J. Porvaznik, "RC3TF, an Augmented Reality CTF: A case study in improving cybersecurity pedagogy for the undergraduate research laboratory," *Proc. 20th Annu. Symp. Inform. Assurance (ASIA '25)*, Albany, NY, pp. 73-82, Jun. 3-4, 2025.
- [31] J. L. Cameron, "William Stewart Halsted: Our Surgical Heritage," *Ann. Surgery*, vol. 225, no. 5, pp. 445-458, May 1997. doi: <https://doi.org/10.1097/0000658-199705000-00002>.
- [32] J. Vozenilek, J. S. Huff, M. Reznec and J. A. Gordon, "See One, Do One, Teach One: Advanced Technology in Medical Education," *Acad. Emergency Med.*, vol. 11, no. 11, pp. 1149-1154, Nov. 2004. doi: <https://doi.org/10.1197/j.aem.2004.08.003>.
- [33] J. M. Hanson, T. L. Trolian, M. B. Paulsen, and E. T. Pascarella. "Evaluating the Influence of Peer Learning on Psychological Well Being," *Teaching Higher Edu.*, vol. 21, no. 2, pp. 191-206, Feb. 2, 2016. doi: <https://doi.org/10.1080/13562517.2015.1136274>.
- [34] D. W. Johnson and R. T. Johnson, "Cooperation and the Use of Technology," In *Handbook of Research on Educational Communications and Technology, 2nd edition*, D. H. Jonassen, editor, pp. 785-811, Mahwah, NJ: Erlbaum.
- [35] E. F. Barkley, C. H. Major and K. P. Cross, *Collaborative Learning Techniques: A Handbook for College Faculty, 2nd edition*, San Francisco, CA: Jossey-Bass.
- [36] C. D. Ryff and C. L. Keyes, "The Structure of Psychological Well-Being Revisited," *J. Personality and Social Psychol.*, vol. 69, no. 4, pp. 719-726, 1995. doi: <https://dx.doi.org/10.1037/0022-3514.69.4.719>.

- [37] "EY Reimagining Industry Futures Study 2024: How can you realize the promises of transformational technologies?" Accessed: Jun. 12, 2025. [Online]. Available: <https://assets.ey.com/content/dam/ey-unified-site/ey-com/en-lu/insights/tmt/documents/ey-luxembourg-reimagining-industry-futures-2024.pdf>.
- [38] "EY Reimagining Industry Futures Study 2025: How can emerging technologies shape industries for sustainable growth and future impact?" Accessed: Jun. 12, 2025. [Online]. Available: <https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/telecommunications/documents/ey-reimagining-industry-futures-02-2025.pdf>.
- [39] "Generative AI for Beginners | Microsoft Learn." Accessed: Jun. 12, 2025. [Online]. Available: <https://learn.microsoft.com/en-us/shows/generative-ai-for-beginners/>.
- [40] "Generative AI: Prompt Engineering Basics by IBM | Coursera." Accessed: Jun. 12, 2025. [Online]. Available: <https://www.coursera.org/learn/generative-ai-prompt-engineering-for-everyone>.
- [41] "Prompt Engineering | Coursera." Accessed: Jun. 12, 2025. [Online]. Available: <https://www.coursera.org/specializations/prompt-engineering>.
- [42] M. Jordan, "Certification: A Stage of Professionalization," *Bulletin Med. Library Assoc.*, vol. 36, no. 2, pp. 108-116, Apr. 1948. PMID: 16016806; PMCID: PMC194717.
- [43] F. Eitel, K-G. Kanz and A. Tesche, "Training and certification of teachers and trainers: the professionalization of medical education," *Med. Teacher*, vol. 22, no. 5, pp. 517-526, 2000. doi: <https://doi.org/10.1080/01421590050110812>.
- [44] T. M. Stinnett, "Accreditation and the Professionalization of Teaching," *J. Teacher Edu.*, vol. 3, no. 1, pp. 30-39, Mar. 1952. doi: <https://doi.org/10.1177/002248715200300108>.
- [45] D. Kallergis, T. Karvounidis, K. Kioskli and C. Douligeris, "Cybersecurity Certification for Professional Training: An Overview," *2025 IEEE Global Eng. Ed. Conf. (EDUCON)*, London, United Kingdom, Apr. 22-25, 2025, pp. 1-8, doi: <https://doi.org/10.1109/EDUCON62633.2025.11016633>.
- [46] K. J. Knapp, C. Maurer and M. Plachkinova, "Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance," *J. Inform. Syst. Edu.*, vol. 28, no. 2, pp. 101-114, Dec. 2017.
- [47] J. E. James and J. Callen, "Cybersecurity Certifications Matter," *Issues Inform. Syst.*, vol. 19, no. 3, pp. 193-201, 2018. doi: https://doi.org/10.48009/3_iis_2018_193-201.
- [48] ISC2, "2024 ISC2 Cybersecurity Workforce Study: Global Cybersecurity Workforce Prepares for an AI-Driven World." Accessed: Jun. 12, 2025. [Online]. Available: <https://edge.sitecorecloud.io/internationalf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/2024-ISC2-WFS.pdf>.
- [49] ISACA, "State of Cybersecurity 2024: Global Update on Workforce Efforts, Resources, and Cyberoperations" Jun. 12, 2025. [Online]. Available: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/reports/isaca-state-of-cybersecurity_2024_1024.pdf.
- [50] ISC2, "2025 Cybersecurity Hiring Trends Report: Why Investing in Entry - and Junior-Level Talent is Key to Building a More Resilient Cybersecurity Workforce," Accessed: Jun. 12, 2025. [Online]. Available: <https://www.isc2.org/Insights/2025/06/cybersecurity-hiring-trends-study>.
- [51] O. Vakulyk, P. Petrenko, I. Kuzmenko, M. Pochtovyi and R. Orlovskiy, "Cybersecurity as a component of the national security of the state," *J. Security & Sustainability Stud.*, vol. 9, no. 3, pp. 775-784, 2020. Available: <https://journals.lka.lt/journal/jssi/article/660/info>.
- [52] Ministry of Public Safety and Emergency Preparedness of Canada, "National Cyber Security Action Plan 2019-2024," 2019. [Online]. Available: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrtr-strtg-2019/ntnl-cbr-scrtr-strtg-2019-en.pdf>.
- [53] L. Kovács, "National cyber security as the cornerstone of national security," *Land Forces Acad. Rev.*, vol. 23, no. 2, pp. 113-120, Jun. 2018. doi: <https://doi.org/10.2478/raft-2018-0013>.
- [54] D. S. Reveron and J. E. Savage, "Cybersecurity Convergence: Digital Human and National Security," *Orbis*, vol. 64, no. 4, pp. 555-570, 2020. doi: <https://doi.org/10.1016/j.orbis.2020.08.005>.