CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 2, No. 1
April 2023
ISSN: 2832-1006

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

2023 Review Board

Educational Cyber Ranges: A Mixed-Method Study of Significant Learning Experiences using Cyber Ranges for Cybersecurity Education

Cheryl Beauchamp
cherbea@regent.edu
Department of Engineering and Computer Science
Regent University
Virginia Beach, VA

Holly Matuscovich
matushm@vt.edu
Department of Engineering Education
Virginia Tech
Blacksburg, VA

Abstract

Cybersecurity breaches and attacks have not only cost businesses and organizations millions of dollars but have also threatened national security and critical infrastructure. Examples include the Ransomware attack in May of 2021 on the largest fuel pipeline in the United States and the February 2021 remote access system breach of a Florida water treatment facility which raised sodium hydroxide to a lethal level. Improving cybersecurity requires a skilled workforce with relevant knowledge and skills. Academic cyber ranges offer virtualized environments that support cybersecurity educators' needs to provide students with a safe, separated, and engaging environment. More and more academic programs utilize cyber ranges due to the perceived benefit of integrating them into their cybersecurity-related programs. The purpose of this study was to understand the educators who were using the Virginia Cyber Range and how they were using them for cybersecurity education. More specifically, the study examined their usage for alignment with a learning taxonomy to verify the usage contributed to successful and significant student learning. Results suggested that high school cybersecurity educators were the primary users. These educators had less formal cybersecurity education and experience compared to cybersecurity educators in higher education. The data also showed that cybersecurity educators primarily used cyber ranges for teaching and learning as opposed to providing feedback and assessment to meet learning goals and objectives.

Keywords: cyber ranges, cybersecurity education, significant learning experiences, integrated course design

1. INTRODUCTION

Ranges are used to practice skills in a controlled environment. Golf driving ranges allow golfers to practice their golf swing before an actual game. A shooting range provides an opportunity to practice with firearms before a qualification test or competition. Similarly, cyber ranges provide a means for organizations to practice penetration testing and incident response in a simulated environment, providing realistic training. The military, government, and private industry use organizational cyber ranges such as the National Cyber Range, the DOD Cyber Security Range, and private cyber ranges such as Raytheon's, IBM's, and Metova's (Smith, 2017). Organizational cyber ranges train their personnel in an operational

context and may include simulated scenarios with realistic networks that mirror the working environment (Brunner et al., 2019). These ranges utilize virtualization for efficiency and cost-effectiveness.

Nonetheless, virtualization software, installation, configuration, and support can be expensive (Brunner et al., 2019). Variations in cyber ranges exist to balance the needs of its users and resources. Specifically, differences in educational cyber ranges exist to meet the challenges of resources and support while also providing specific educational needs. Compared to organizational cyber ranges, academic facing cyber ranges in cybersecurity education are relatively new. The purpose of this study is to contribute to research on educational cyber ranges and cybersecurity education by describing who is using the Virginia Cyber Range (VaCR) for educational purposes and how they are using it.

For cybersecurity educators, a cyber range is a safe, virtual environment for activities that support cybersecurity-related hands-on learning (Darwish et al., 2020). Cybersecurity educators will most likely use cyber ranges in their classrooms to aid instructional content or assessment (NIST, 2018). They may also use cyber ranges outside of the classroom for professional development (PD) and enrichment activities (Beauchamp et al., 2020). A cyber range supports efforts to provide cybersecurity education with engaging hands-on exercises and labs to gain proficiency in a safe, virtual environment. Since the implementation of cyber ranges for educational purposes in academic settings is relatively recent, there is a need to explore and describe educational cyber ranges to develop theory and understand how these academic cyber ranges support cybersecurity educational efforts.

Accordingly, this research focuses on a single cyber range, the VaCR. Understanding how the VaCR supports teaching and learning may be valuable to others interested in investing in an educational cyber range. The results of studying the VaCR may transfer if future locations decide the approach is fitting for their needs (Tracy, 2010). The VaCR is an advantageous location to explore educational cyber ranges. Its purpose is specified for education, its cloud-based design increases its accessibility, and its multi-university collaboration provides an abundance of cybersecurity education resources.

The purpose of this study was to describe who are the educators using cyber ranges for cybersecurity education and how they are using them to create significant cybersecurity learning experiences from the educator's perspective. Using Fink's Significant Learning Experience (SLE) taxonomy (2013) as a theoretical lens, the study addresses the following research questions:

- Who are the educators using the VaCR for educational purposes?
- How is the VaCR used for cybersecurity education?

The analysis described how the VaCR is used through the perspective of its registered educators to provide an understanding of how cyber range resources are used by cybersecurity educators and who are the educators using them to support cybersecurity education.

2. CYBER RANGES: APPROACHES AND CURRENT USAGE LANDSCAPE

A single definition of cyber ranges does not exist as they have varying types, users, and purposes. Understanding cyber ranges in cybersecurity education requires understanding the types, the users, and the purposes. Additionally, the technological capabilities and approaches have changed through the years due to advancements in hardware and software capabilities, dating some of the prior research studies (Yamin et al., 2019). Previous studies tend to focus on a specific cyber range. They have not included an understanding of how cyber ranges are used for cybersecurity education from the perspective of cybersecurity educators.

A list of known cyber ranges and their capabilities is provided in Appendix A. This list and descriptions of cyber range providers, users, objectives, type of infrastructure, and deployment platforms was compiled from several prior studies (Babcock, 2019; Circadence, n.d.; Davis & Magrath, 2013; Georgia Technology Authority, n.d.; Hayman, 2019; National Cyber Warfare Foundation, 2019; Priyadarshini, 2019; Yamin et al., 2019). An Australian cyber range survey (Davis & Magrath, 2013) study compiled information to describe the approaches and functionality of existing cyber ranges to assist organizations when making informed decisions regarding cyber ranges. Their approach to cyber range classification was by who used the cyber range and the cyber range approach. The study is considered dated compared to current cyber range technology advancements and tools (Yamin et al., 2019). Yamin's study, conducted six years later, addressed the need for a more current study.

Yamin et al.'s literature review addressed the gap in research as previous studies were considered outdated or focused too specifically on one domain and did not provide a general understanding of cyber range systems (2019). The objectives of the review included identifying and classifying the cyber range functionality; evaluating cyber range approach and architecture model; classifying cyber range application as either training or testing; and identifying methods to assess different cyber ranges against a standard. The means for evaluation included the cyber range scenarios, functions, and tools.

These prior studies contribute to our understanding of the current cyber range landscape by providing definitions and categorizations. However, little is known about how educators use cyber ranges for cybersecurity education. As seen in Appendix A, there were nine academic providers of Cyber Ranges as of 2021. Only three academic cyber range providers identified education as their single objective. Although both the VaCR and the Arkansas Cyber Range limited their participants to academic participants, the VaCR provided Cloud access. A description of cyber range providers, users, objectives, type of infrastructure, and deployment platforms contribute to understanding the variances of cyber ranges prior to singling in on cyber ranges that are used for cybersecurity education. A description of each classification contributes to understanding who is involved with cyber ranges, their history, participants, stated objectives, and the characterization of their operations.

3. THEORETICAL LENS

Recognizing that educators with varying situational factors may apply different teaching activities and assessments to meet cybersecurity learning goals, this study used Fink's Integrated Course Design (ICD) framework (2005) to explore how Virginia educators used the VaCR for significant student learning experiences. Several prior studies have applied Fink's Significant Learning Experience taxonomy and ICD framework principles to courses in several disciplines. These include a health policy course (Krueger et al., 2011), a psychology program course (Fallahi, 2008), a nursing program course (Marrocco, 2014), and a sustainability engineering course (Apul & Philpott, 2011). These studies used the principles to redesign existing courses and evaluate the changes against Fink's Significant Learning Experiences taxonomy. This study differs in that it investigates existing elements in current educational practices versus studying their intentional implementation as in these prior works.

According to Fink's model, educators' situational factors influence the teaching and learning activities, the feedback, and the assessments integrated within their courses to meet the learning goals (Fink, 2005). Fink's work claims that this ICD contributes to significant learning experiences for students (Streveler et al., 2012; Fink, 2013). Significant learning consists of six dimensions of learning categorized as Foundational Knowledge, Application, Integration, Human Dimension, Caring, and Learning How to Learn (Fink, 2013). These categories interact to contribute to significant learning.

These six categories of significant learning formulate the learning goals in the ICD framework. The components of ICD, including the learning goals, situational factors, teaching and learning activities, and feedback and assessment, are interconnected. The learning goals provide the means for formulating the appropriate feedback and assessment procedures. These, in turn, provide the necessary understanding to select effective teaching and learning activities. Foundational to these components are the situational factors that may impact them.

Situational factors may affect decisions regarding the learning goals, the feedback and assessment, and the teaching and learning activities. These factors include the context of the teaching and learning situation, the nature of the subject, the characteristics of the learner and teacher, and any particular pedagogical challenges. Pedagogical challenges are situations that may present challenges to the students or the educator and the opportunity for significant learning (Fink, 2013).

Using the ICD components to explore how educators used cyber ranges, a special pedagogical challenge (Fink, 2013), provided an encompassing understanding of how educators use cyber ranges for significant cybersecurity learning. The findings described how they used the cyber range to support teaching and learning activities, provide feedback to students, and assess students' learning.

4. METHODS

This study drew upon both quantitative and qualitative data to understand the VaCR registered educators and how they used the VaCR for cybersecurity education. This study

contributes to a larger case study to understand cyber ranges in cybersecurity education through the educator and student perspectives. The VaCR was the unit of analysis for this study. The data sources were educator responses to a questionnaire and data sources from the VaCR, such as their website and traffic data. This study was conducted in accordance with the university human subject's research requirements and necessary ethical considerations to protect the educator participants.

Case Site Description

The VaCR was created in 2016 with the mission to enhance cybersecurity education and increase the number of students entering the cybersecurity workforce (Virginia Cyber Range, n.d.) Since the VaCR was designed and developed specifically for education, the data associated with its users, usage, and resources contribute to educational purposes. This academic focus enables findings from this study to correlate educational efforts related to the cyber range compared to a cyber range that may have mixed users, usage, and resources.

The VaCR is cloud-based, accessible via a web portal. Users are not required to purchase supporting software, configure hardware, or pay expensive access fees. Its resources are openly available to Virginia public educational institutions. The registered users are students and faculty in over 200 high schools, community colleges, and universities. According to the cyber range registration data provided by the Communications and Development Manager for the VaCR, over half of the VaCR registered educators in 2020 were high school educators (Lawrence-Kuether, 2020). Accessibility is supported by over 50,000 deployed virtual machines (Virginia Cyber Range, n.d.). The VaCR approach of hosting their cyber range in the cloud provides rapid scalability and low-cost investment with fees associated with usage. The cyber range is not location-dependent and is accessible globally via a user login through their web portal.

As of 2021, the VaCR is advised by members from public higher education institutions in Virginia that have been nationally designated as Centers of Academic Excellence in Cybersecurity by the National Security Agency and the Department of Homeland Security. There are 17 colleges and universities with this designation on the advisory committee, and this status continues to expand as more public Virginia colleges become designated. Through this multi-college and university partnership, the VaCR provides an extensive courseware repository of courses, labs, workshops, lessons, and environments (Raymond, n.d.).

Data Collection

The data sources were responses to an anchored open-ended (AOE) questionnaire, the VaCR website, and traffic data provided by the administrators of the VaCR to gather resource usage. The primary data source, the AOE questionnaire, included in Appendix B, was sent to the registered educators of the VaCR to obtain a sample of cybersecurity educators. there were 85 educators who participated in the study. Since the study did not require personal educator identification, identifiable information such as the participants name was not included to protect the participant's identity. Communication with the VaCR administrators provided traffic data reports.

Sampling Plan

This study used a purposive non-probability sampling approach to study who uses the VaCR and how they use it (Trochim, 2006). The reason for purposefully selecting the Virginia/US Cyber range was its ability to meet specific criteria to include its focus on cybersecurity education versus the other cyber ranges included in Appendix A. The Virginia Cyber Range is only accessible to educators via required registration. The questionnaire was sent to all the registered members to provide a means to obtain a diverse, heterogeneous sampling (Trochim, 2006). Due to the small population of VaCR registered educators, this study used follow-up emails and a gift card drawing incentive to encourage higher response rates. Although 85 educators contributed different levels of questionnaire responses, 70 of them reported using the VaCR during the 2020 – 2021 academic year.

AOE Questionnaire and Traffic Data

An AOE questionnaire uses the responses to closed-ended questions as foundations (or anchors) for accompanying responses to open-ended questions. Lee & Lutz (2016) found that AOE questions provided the ability to sort a large number of responses more quickly than open-ended questions and more accurately than closed-ended questions. The instrument for this study used closed-ended questions to capture information regarding who the VaCR registered educators were, what they taught, and which VaCR resources they used. The instrument also included open-ended questions to further record information to corroborate and explain participants' answer choices for the closed-ended questions. For example, in addition to recording which VaCR resources they used for assessment, respondents were asked to provide examples of

how they used the cyber range to support their assessment efforts.

A prior conference panel discussion with four Virginia high school cybersecurity educators (Beauchamp et al., 2020) provided initial insight regarding how they used the VaCR. This insight contributed to the initial design of the instrument questions. Additionally, two VaCR educators reviewed the instrument and provided their feedback for content validity, clarity of the questions, and overall ease of completing the instrument.
The VaCR traffic data was used to corroborate and triangulate the questionnaire responses regarding the VaCR resources educators utilized.

Analysis
The open-ended responses to the AOE questionnaire were analyzed qualitatively using in vivo and descriptive coding (Miles et al., 2020; Saldana, 2016). The coding used the ICD components of teaching and learning, assessment and feedback, and significant learning goals as the lens to explore how educators use cyber ranges. Appendix C includes partial tables for each of the coding steps.

A fellow qualitative researcher cross-checked codes using the developed codebook (Creswell & Creswell, 2018). Their review and coding addressed inter-rater reliability (Creswell & Poth, 2018).

Analysis of the closed-ended questions for educator information included who used the VaCR and how they used it. These traffic data reports were analyzed to determine which resources were utilized, the time duration of use, and the frequency of use. The VaCR website described the available educational resources. The traffic report data and resource description were used to triangulate questionnaire data.

5. FINDINGS

In addressing the first research question, although the stated mission of the Virginia Cyber Range is to enhance cybersecurity education for students at the high school and post-secondary levels (Virginia Cyber Range, n.d.), results showed that high school educators are the primary users of the VaCR for cybersecurity education, and they are predominantly male, with 67.4% of the participants identifying as male. This is a higher percentage compared to the national percentage of male computer science high school educators. Although cybersecurity educators are primarily Career and Technology Educators, some educators may also be certified as Computer Science teachers. According to an estimate that was verified against the Bureau of Labor and Statistics, 53.6% of high school computer science teachers identified as male (Zippia Careers, 2021). Additionally, results showed that high school educators had less formal technical education, experience, and certifications than those in higher education, but they utilized online workshops more than their counterparts. Those who taught cybersecurity for the first time were all high school educators. For purposes of this study, these first-time cybersecurity educators are referred to as novices.

Educators who use VaCR for Cybersecurity Education
VaCR educators are primarily high school educators. As seen in Figure 1, high school educators make up more than half (52%) of the educators who use the VaCR. The other half were higher education educators at community colleges (17%), universities and colleges (28%), and educators who did not identify their level of teaching (3%).

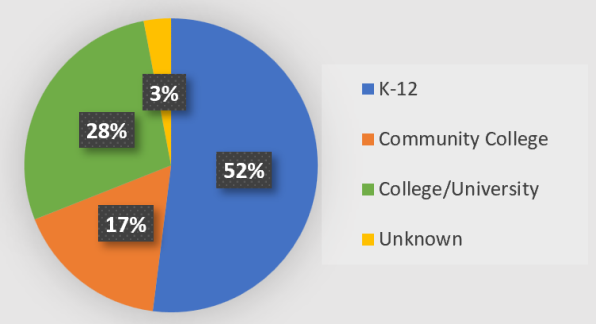

Figure 1: VaCR Registered Virginia Educators

The educators who responded to the study reflected a similar composition of instruction-level as the overall population of VaCR registered educators, as seen in Figure 2.

VaCR educators teach technical, business, and STEM courses. Virginia educators who used the VaCR in 2020-2021 taught technology courses: Cybersecurity Fundamentals, Introduction to Programming, Computer Networks, Digital Forensics. The high school educators also taught business, science, and math courses. A list of courses taught in 2020 - 2021 is provided in Appendix D.

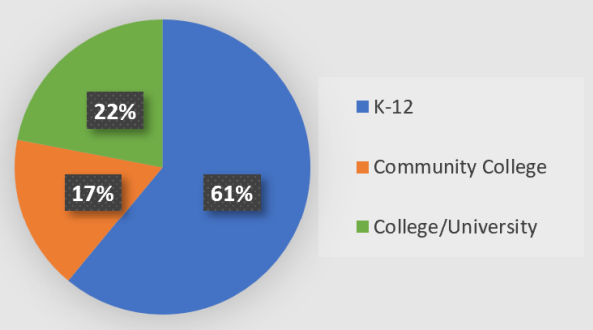

Figure 2: Breakdown of Study Participants

46 of the 70 participants who used the VaCR provided gender information. These educators primarily identified male (67%) versus female (33%). Figure 3 reflects the gender representation at the high school, community college, and university/college levels from those who reported gender identification information. The question format followed engineering education recommendations for more inclusive approaches to collecting demographic data such as providing a gender continuum (Fernandez et al., 2016). Utilizing their recommended approach, the question stem uses gender, and the choices are actually for participant sex, so we report the results as the question was asked.

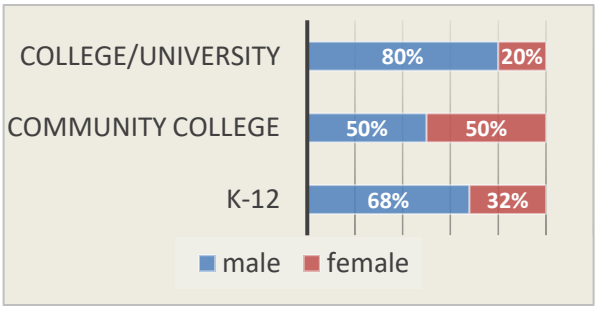

Figure 3: Gender of VaCR Educators

Educators were primarily White (59%), but others also identified as Black or African American (9%), Hispanic, Latino, or Spanish origin (4%), or Asian or Asian American (2%) as depicted in Figure 4.

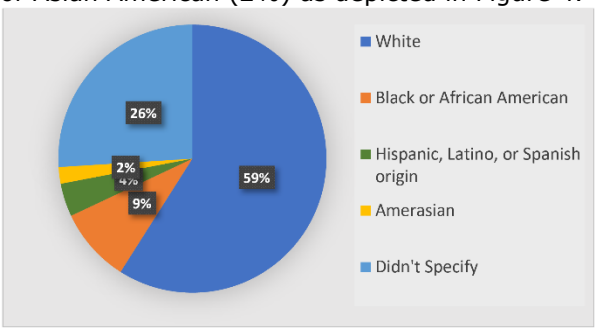

Figure 4: Racial Groups of VaCR Educators

High school educators had less professional technical experience, industry certifications, and formal academic courses in cybersecurity than higher education educators but more involvement in Communities of Practice (CoPs), Informal Learning Communities (ILCs), and other sources for preparation; primarily the GenCyber program. They and community college educators also utilized online workshops. Six high school educators identified as novices; they taught a cybersecurity course for the first time in 2020 - 2021. There were no novices at the community college or the university/college level. The reported prior education, preparation, or experience are shown in Figure 5.

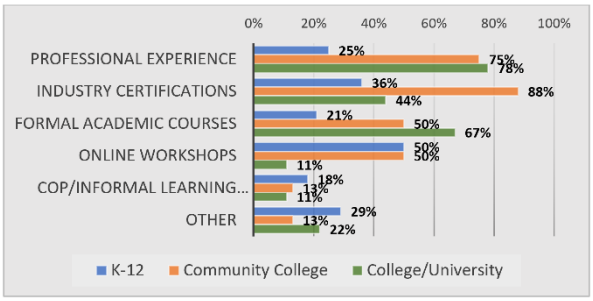

Figure 5: Prior Preparation and Experience of VaCR Educators

68% of high school cybersecurity educators stated they held a Virginia education teaching license. Currently, cybersecurity licensure is unavailable in Virginia. Many educators reported having business and technology licensure as cybersecurity-related courses are offered in the Career and Technical Education programs. Other educators reported licensure in Computer Science, Physics and Math, or Business & Marketing. One educator listed their licensure in Business, English, Physical Education, and Social Sciences.

VaCR usage for Cybersecurity Education

The results regarding the second research question show that educators primarily use the VaCR for teaching and learning activities. Although the VaCR was not currently or widely used for providing feedback and assessment, educators shared that they would like to use the VaCR more when they have time and understanding of how to utilize it for effective feedback and assessment. The results also demonstrated that educators who used the VaCR provided significant learning experiences as their usage addressed the six constructs of the significant learning goals.

Results showed that educators primarily use the VaCR for its hands-on labs and its CTF tool (See Figure 6). Some educators created their own labs,

but others reported using Brigante, Metasploit, Kali Linux and Windows, Linux Intro, labs related to password cracking and auditing, Ubuntu, and labs that supported tools such as Nmap, JTR, Wireshark, Snort, Mcrypt, and DVWA for scanning. Other resources included instructional information, curriculum development, and operating system virtual machines.

A lack of awareness of the other resources may be a reason for low reported usage as one high school novice educator shared, "I was unaware of any videos, weekly workshop series, etc. I went into teaching Cybersecurity with no preparation, few materials, and was advised by the previous teacher to join the cyber range."

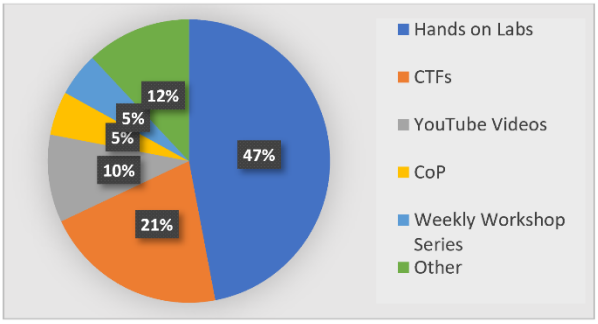

Figure 6: VaCR Resource Usage

Teaching and Learning Activities

Educators at all instructional levels reported similar usage of the VaCR for teaching and learning. The accessible and ready-to-use environments, such as the Kali Linux, Windows Virtual Machine, Ubuntu, and Brigante, provided online accessibility for students to work with cybersecurity tools safely.

The accessible environment also provided educators the means for their students to use cybersecurity tools and operating system commands in a safe and protected environment. The ability to apply and practice using tools, such as Wireshark and Linux commands, they learned about in class was another way educators used the VaCR to reinforce their teaching and learning activities. Although some educators created their own labs in the VaCR environment, others reported using the existing labs and lessons which mapped to their learning objectives.

Educators also used the CloudCTF tool for teaching and learning. Some utilized it as homework assignments, others as an assessment tool, while still others as a demonstrative tool. Appendix E provides excerpts from educators regarding their usage of the VaCR for teaching and learning activities.

Feedback and Assessments

Educators at all instructional levels shared using the VaCR for formative assessment, summative assessment, and feedback. However, they used it primarily for summative assessment purposes. Educators used the labs, working environments, and CTFs to assess student learning. Some shared that they did not use the VaCR for feedback, that although they did not currently use the VaCR for assessment or feedback, they plan to do so in the future. As stated by one experienced college-level educator, "I do not currently use it in my assessments right now but will eventually use it in the future." Appendix F provides excerpts from educators regarding their usage of the VaCR for feedback and assessments.

Learning Goals

All six dimensions of Fink's (2013) Significant Learning Goals were evident from educators using the VaCR for cybersecurity education. Although educators did not expressly state their teaching efforts aligned with the goals, their descriptions of how they used the VaCR demonstrated their teaching efforts supported their students' abilities to meet these learning goals.

Foundational Knowledge: Students remember and build an understanding of cybersecurity information by using the labs, environment, and CTFs, both in and out of class. This usage provides means for students to build their foundational cybersecurity knowledge.

Application: Students learn how to apply new learning via the VaCR hands-on activities and environments. This hands-on application requires critical, creative, and practical thinking skills and time management and content knowledge to further their skills. Using the labs, environment, and CTFs, students learn new actions: new skills and ways of thinking. For example, this educator shared that he used the VaCR "for my labs and homework to give the students a better source for practicing using the tools and other information involving the fundamentals and frameworks."

Integration: Working with VaCR resources, students connected various subjects such as programming, networks, and cybersecurity fundamentals as well as group or team skills and project management. Through this integration, students connect various subject areas and learning experiences, including team/group work activities. One educator stated he used the "cyber range environment for application of network reconnaissance, footprinting, and enumeration principles" and for "application of firewall, IDS

configuration principles and public key cryptography concepts."

Human Dimension: students build new connections with themselves and others when they apply their course knowledge in labs that provide hands-on practice and opportunities to work with others. For example, one educator shared that although his students had individual assignments, he encouraged them to work with each other to learn different strategies for achieving the learning objectives of the assignment, "students are permitted to network with their class peers on the assignments. I find that the students learn by discussing options & strategies for achieving objectives with their peers."

Caring: Educators shared students experienced positive engagement when using the VaCR. Educators also shared that this positive engagement reinforced their students' interest in cybersecurity using the cyber range. Students develop interest or value for cybersecurity with the positive and active learning engagement when using the VaCR. According to Fink, "the development of new interests, feeling, and values" contribute towards the caring component of significant learning (2013, p.83). An educator shared that he uses the VaCR as a reward, "students enjoy the gamification aspect of the CTFs," while another educator shared that he finds using the VaCR rewarding due to his students' positive engagement using the VaCR, "Their excitement of successfully completing the [Denial of Service] lab was contagious."

Learning to Learn: The labs, environment, and CTFs also provide students an opportunity to become better cybersecurity students and self-directed learners. One educator stated, "My students like the [Virginia Cyber Range] range as a self-directed tool that gives them a break from my lectures."

Limitations

As with all studies, this research has limitations. They do not invalidate the findings but should be considered. The population of VaCR registered educators was purposefully selected to study the VaCR; therefore, the transferability of findings from the VaCR to another cyber range may be limited. However, the "fittingness" of the findings to the reader's own experience and situations (Krathwohl, 2009, p. 350) was supported through rich and detailed descriptions. Additionally, VaCR educators who participated did so voluntarily. Thus, self-selection bias might exist, and the sample may skew towards educators who had strong opinions towards using cyber ranges. Therefore, this study may not represent all views and does not claim to do so.

Another limitation is the small sample size due to the small population of VaCR registered educators. These VaCR users are mostly high school level cybersecurity educators, while other cyber ranges may have more users at the post-secondary level. The low response rate was an additional limitation which may have been due to varying factors, including the timing of the questionnaire in the academic school year, or due to the impact of COVID-19. Again, this study does not make claims of generalizability but instead contributes as an exploratory study of educators who use the VaCR and how they use the VaCR for cybersecurity education.

6. DISCUSSION & IMPLICATIONS

Discussion

Findings from this study support the usage of cyber ranges for cybersecurity education to provide Significant Learning Experiences. Results show that VaCR supported the three components of the ICD framework, as seen in Figure 7. Educators shared that the virtual environment is a safe and accessible environment for users to apply concepts presented in class to develop application skills and reinforce student understanding of cybersecurity-related concepts. The ready-to-use and customizable labs, lessons, and CTFs provided hands-on practice that contributed to teaching and learning activities. The VaCR also provided a means for feedback and assessment, though some educators did not report widely utilizing this capability yet. Nonetheless, educator usage of the VaCR also reflected the ability to address all six dimensions of Fink's Learning Goals for providing Significant Learning Experiences (2013).

However, educators shared a lack of awareness of the different VaCR resources to assist their full usage of the VaCR. Some educators were assigned to teach cybersecurity and were not prepared to do so. Advised to utilize the VaCR, they were left to learn how to use it independently.

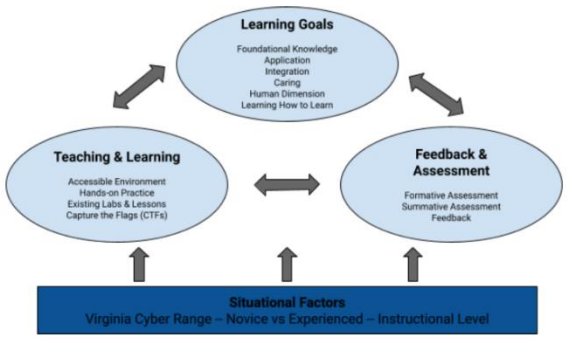

Figure 7: Educators' Usage of VacR Alignment with Fink's Significant Learning Experiences and ICD

Over half of the educators using the VaCR were high school educators with limited prior preparation or experience in cybersecurity education. These high school educators teach STEM, business, and technical courses as their primary teaching disciplines, as reflected in their state teaching licenses. Although the VaCR resources include workshops and videos to assist educators throughout the year, they were not widely used, perhaps because educators were unaware of these resources or did not have time for PD during the school year. High school educators shared they are more likely to engage in PD opportunities offered during the summer. They reported utilizing online and summer workshops for further PD.

Implications

The primary implication from this study is that cyber ranges in cybersecurity education support efforts to provide significant learning experiences. However, the integration will have limited success if the educators are not provided the necessary training and resources to support their efforts to utilize these ranges. Cybersecurity and cyber range stakeholders need to create a curriculum, instructor guides (w/solutions), and content that maps to cybersecurity learning objectives. PD programs should include awareness of these resources and how to use them. Cybersecurity and cyber range stakeholders need to create and facilitate PD offerings for novice educators, and they need to collaborate on associated research efforts.

Additionally, secondary education administrators who provide cybersecurity-related courses in their schools can support cyber range integration in those courses knowing the integration supports significant learning. However, this integration requires supporting cybersecurity educators with time and resources to pursue cybersecurity and cyber range-related PD. Educators can integrate cyber ranges in their cybersecurity-related courses with administrative support and attend cyber range and cybersecurity education PD opportunities.

Although the VaCR currently provides additional educator support resources to include Workshops Series and YouTube videos, findings from this study show educators did not report utilizing these resources. Further research is necessary to understand why VaCR educators did not widely use these resources. This understanding supports cyber range developers and stakeholders' ability to provide and update resources from which their educator users would benefit.

Continued research collaboration of all the stakeholders will also provide a further understanding of cyber ranges in cybersecurity education. Future studies include comparing usage by instructional levels and by experience level. Follow-up studies regarding differences in educator cyber range usage based upon gender, size of class enrollment, novice vs. experienced educator, core subject area, and prior preparation can use the questionnaire instrument from this study. These other areas are identified as situational factors for designing significant learning experiences – specific context of the teaching and learning situation and the characteristics of the educator (Fink, 2013). Future studies may include looking at some of these other situational factors and how they are related to using cyber ranges.

7. REFERENCES

Apul, D. S. & Philpott, S. M. (2011). Use of outdoor living spaces and fink's taxonomy of significant learning in sustainability engineering education. Journal of Professional Issues in Engineering Education and Practices, 137(2), 69-77. doi:10.1061/(ASCE)EI.1943-5541.0000051

Babcock, S. (2019) Economic leaders paid a visit to Maryland cyber centers. Technically Media. https://technical.ly/baltimore/2019/02/21/georgia-economic-leaders-paid-a-visit-to-maryland-cyber-centers/

Beauchamp, C., Frey, E., Marden, J., Rice, K., & Riggleman, K. (2020). At the center of cybersecurity education: The Virginia cyber range. Virginia Cybersecurity Education Conference, July 27-28, 2020. (Virtual).

Brunner, R., Oh, S. K., Ramirez, J., Houck, P., Stickney, N., & Blaine, R. (2019). Design for an educational cyber range. Proceedings of

the 6th Annual Symposium on Hot Topics in the Science of Security. Nashville, TN. (April 1-3, 2019).

Circadence. (n.d.) Helping cyber professionals prepare and protect. Circadence. https://www.circadence.com/company/about/

Creswell, J. W. & Poth, C. N. (2018). Qualitative inquiry & research design: Choosing among five approaches (4th ed.). Thousand Oaks, CA: Sage.

Darwish, O., Stone, C. M., Karajeh, O., & Alsinglawi, B. (2020). Survey of educational cyber ranges. In: Barolli L., Amato F., Moscato F., Enokido T., Takizawa M. (eds) Web, Artificial Intelligence and Network Applications. WAINA 2020. Advances in Intelligent Systems and Computing, 1150. Springer, Cham. https://doi.org/10.1007/978-3-030-44038-1_96

Davis, J., Magrath, S. (2013). A survey of cyber ranges and testbeds. Defense Science and Technology Organization Edinburgh (Australia) Cyber and Electronic Warfare Division. Dicke A-L, Safavian N. & Eccles, J.S. (2019) Traditional Gender role beliefs and career attainment in STEM: A gendered story? Frontiers in Psychology,10(1053). doi: 10.3389/fpsyg.2019.01053

Fallahi, C. R. (2008). Redesign of a lifespan development course using fink's taxonomy. Teaching of Psychology, 35(3), 169-175. doi: 10.1080/00986280802289906.

Fernandez, T., Godwin, A., Doyle, J., Verdin, D., Boone, H., Kirn, A., Benson, L., & Potvin, G. (2016). More comprehensive and inclusive approaches to demographic data collection. School of Engineering Education Graduate Student Series. http://docs.lib.purdue.edu/enegs/60

Fink, L. D. (2003). What is significant learning. University of Oklahoma Significant Learning Website, Program for Instructional Innovation at the University of Oklahoma.

Fink, L. D. (2005). Integrated course design. The IDEA Center. https://www.ideaedu.org/Portals/0/Uploads/Documents/IDEA%20Papers/IDEA%20Papers/Idea_Paper_42.pdf

Fink, L. D. (2013). Creating significant learning experiences: An integrated approach to designing college courses. San Francisco, CA: Jossy-Bass.

Georgia Technology Authority. (n.d.) Georgia Cyber Center. Georgia Technology Authority. https://gta.georgia.gov/georgia-cyber-center

Hayman, S. (2019). Cyber range: New platform and degree readies students for cyber defense. University of Central Arkansas Magazine. https://uca.edu/magazine/cyber-range/

Krathwohl, D. R. (2009). Methods of educational and social science research: The logic of methods. (3rd ed.) Long Grove: Waveland Press.

Krueger, K. P., Russell, M. A., & Bischoff, J. (2011). A health policy course based on fink's taxonomy of significant learning. American Journal of Pharmaceutical Education, 75(1), 14.

Lawrence-Keuther, M. (2020, July 6). Personal communication.

Lee, W. C., & Lutz, B. D. (2016). An anchored open-ended survey approach in multiple case study analysis. Paper presented at the ASEE Annual Conference and Exposition, New Orleans, LA.

Miles, M. B., Huberman, A. M., & Saldana, J. (2020). Qualitative data analysis (4th ed.). SAGE Publications.

National Cyber Warfare Foundation. (2019) Cyber ranges. National Cyber Warfare Foundation. https://cwr.dev/ranges/

National Institute of Standards and Technology, (2018, August 27). NIST general information. NIST. https://www.nist.gov/National Institute of Standards and Technology. (2018, February 15). Cyber Ranges. NIST. https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf

Priyadarshini, I. (2019). Features and architecture of the modern cyber range: A qualitative analysis and survey. [Unpublished Master's thesis]. University of Delaware. http://dspace.udel.edu/bitstream/handle/19716/23789/Priyadarshini_udel_0060M_13323.pdf?sequence=1&isAllowed=y

Raymond, D. (n.d.) Using cyber ranges for cybersecurity education. Virginia Cyber Range. https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/24.pdf

Saldana, J. (2016). The coding manual for qualitative researchers. SAGE Publications.

Smith, Jim III. (2017). Experiential learning via cyber ranges. National Institute of Standards and Technology (NIST) Federal Information Systems Security Educators' Association (FISSEA) Awareness – Training – Education. https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/6.pdf

Streveler, R. A., Smith, K.A., & Pilotte, M. (2012). Aligning course content, assessment, and delivery: Creating a context for outcome-based education. In K. M. Yusof, N. A. Azli, A. M. Konlin, S. K. S. Yusof, & Y. M.Yusof (Eds.), Outcome-based science, technology, engineering, and mathematics education: Innovative practices, 1-26. IGI Global.

Tracy, S. J. (2010). Qualitative quality: Eight "Big-Tent" criteria for excellent qualitative research. Qualitative Inquiry,16(10), 837-851.

Trochim, William M. (2006). The Research Methods Knowledge Base, 2nd Ed. at URL: http://www.socialresearchmethods.net/kb/.

Virginia Cyber Range. (n.d.) About. Virginia Cyber Range. https://www.virginiacyberrange.org/about

VMware. (2006). Virtualization overview: VMware white paper. VMware. https://www.vmware.com/pdf/virtualization.pdf

Yamin, M. M., Katt, B., & Gkioulos, V. (2019). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88. Elsevier.

Zippia Careers. (2021, December 14). Computer science teacher demographics. Retrieved March 10, 2022, from https://www.zippia.com/computer-science-teacher-jobs/demographics/#gender-statistics

Editor's Note:

This paper was selected for inclusion in the journal as an EDSIGCON 2022 Meritorious Paper. The acceptance rate is typically 15% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2022.

APPENDIX A
Cyber Ranges Providers, Participants, Stated Objectives, Infrastructure & Deployment

Cyber Range	Providers	Stated Objectives	Participants	Infrastructure Type	Deployment Type
University of Maine at Augusta	Academic	MDI, ED, E&C	All users	Public	Cloud & VPN
Virginia	Academic	ED	Students & Academic researchers	Public/Private	Cloud Only
Michigan	Academic	MDI, ED, E&C	All users	Federated/Public/Private	Cloud & VPN
University of Delaware	Academic	ED	All users	Private	No Cloud
Regent University	Academic	MDI, ED, E&C	All users	Private	Cloud & VPN
Wayne State	Academic	MDI, ED, E&C	All users	Federated/Public/Private	Cloud & VPN
Arkansas	Academic	ED	Students	Public	No Cloud
Georgia	Academic	MDI, ED, E&C	All users	Public/Private	Cloud & VPN
Cyber Warfare Range (Arizona)	Academic	OS	All users	Public/Private	Cloud & VPN
National (DARPA)	Government	MDI, ED, E&C	All users	Federated	Cloud & VPN
Department of Defense (DOD)	Government	MDI	Organizations & Professionals	Federated	Cloud & VPN
NATO	Government	MDI	Organizations	Federated	Cloud & VPN
IBM	Commercial	E&C	Organizations & Professionals	Private	Cloud Only
Cisco	Commercial	ED & E&C	All users	Public/Private	Cloud Only
Raytheon	Commercial	E&C	Organizations & Professionals	Federated	Cloud & VPN

Baltimore	Commercial	E&C	Organizations & Professionals	Public/Private	Cloud & VPN
Florida	Commercial	MDI, ED, E&C	All users	Federated/Public/Private	Cloud Only
Cyberbit	Commercial	SP	All users	Private	Cloud & VPN
Circadence	Commercial	SP	All users	Private	Cloud Only

(Abbreviations in Stated Objectives: **MDI**: Military, Defense, and Intelligence, **ED**: Education, **E&C**: Enterprise and Commercial, **SP**: Source Provided, **OS**: Open Source)

Providers

The three types of providers are classified as government, commercial, and academic. Government providers include military, defense, and other government agencies. Commercial providers include industry related organizations, and academic providers include both private and public academic institutions.

Participants

Participants are cyber range users. These include organizations, professionals, students, and academic researchers.

Objectives

Several different utilization purposes were identified to classify cyber range operation objectives. The most common include the following Military, Defense, and Intelligence (MDI); Education (ED), Enterprise and Commercial (E&C), Source Provider (SP), and Open Source (OS).

MDI cyber ranges stated objective is to combat cyber terrorism and defend our national cyber-infrastructure. According to Davis and Magrath, the United States Air Force was a leader in cyber ranges, having used cyber ranges since 2002 (2013).

Priyadarshini claims the educational objective to utilize cyber ranges was more recently realized in 2015. Educational cyber ranges, EDs, meet educational needs for training, certification preparation, and research. However, Davis and Magrath cite earlier academic endeavors to simulate the effects of network attacks for training purposes to include University of Illinois' Real Time Immersive Network Simulation Environment (RINSE) in 2006 and Rochester Institute of Technology's ARENA simulation software in 2007 which modeled "computer networks and intrusion detection systems (IDS) and then applies simulated attacks" (2013, p. 9).

Organizations utilize E&C cyber ranges to not only train their employees, but to address vulnerabilities and threats to their digital infrastructure. IBM's cyber range, launched in 2016, is considered the first commercially available cyber range and uses live malware to test security (Priyadarshini, 2019).

Source providers offer cyber range solutions to meet various objectives. They offer simulation centers for training and testing services.

Finally, OS cyber ranges meet different objectives, to include training and testing for the various types of users. They differ from others in that they are open, free environments that encourage the users to contribute to the available resources to include war games and real opponent challenges.

Infrastructure Type

Three primary associations were identified for classifying based upon the type of infrastructure to include Federated, Private, and Public. These classifications are based upon funding support. Some cyber ranges belong to multiple infrastructure groups as they are supported through a collaborative effort of these types of organizations.

Deployment Platforms

Cyber Range variations can be broadly classified into four main platforms (Darwish et al., 2020; Raymond, D., n.d.) to meet the needs of its users. These types include Local Network Virtualizations, Hosted Virtualizations, commercial-hosted offerings, and Cloud-hosted offerings.

Local Network Virtualization (Raymond, D., n.d.) supports customization of the environment, through network virtualization software, to build various network models and labs for onsite training. These cyber ranges have limited scalability and require a significant financial investment not only for deployment on the site's infrastructure but additionally for the costs associated with ongoing maintenance and administrative support.

Hosted Virtualization (VMware, 2006) supports smaller environments. Virtualization software, such as VMWare or VirtualBox is used to create the training environment on the client machine. Although free virtualization software options exist, the client machine requirements to effectively run the virtualization adds considerable costs.

Commercial-hosted offerings support large and small learning environments. They provide courseware, labs, and pre-configured environments for students to access via a web portal. Most include registration fees based on the duration of registration time or upon specific course registration. The courseware tends to focus on industry certification preparation as they partner with various organizations to include Cisco, Palo Alto, and CompTIA.

Cloud-hosted offerings also support both large and small learning environments. They focus on cybersecurity academic support needs, providing courses, labs, workshops, videos, scenario simulation exercises, and both off-the-shelf (OTS) and customizable Capture the Flag (CTF) competitions (Beauchamp et al., 2020).

APPENDIX B
Anchored Open-Ended Questionnaire for Educators

Please provide the following information regarding your teaching experience and background. Complete one row for each course you have taught within the past five years. Please use the text box to provide the name of the specific course. Space is provided for up to six courses.

Course	Currently teaching or have taught this in an academic year?	Number of times teaching this subject in the past five years	If currently teaching, the number of students enrolled in this course across all sections you teach/taught during this academic year.	Average class size per section	Grade level (elem, middle, high, college)

1. Which of the following contributed to your preparation for teaching cybersecurity? Check all that apply.
    - Professional experience (Please state the type of profession and years of experience.)
    - Industry certifications (please list the certifications and year of acquisition)
    - Online workshops
    - Formal academic course(s) related to cybersecurity (please list the courses).
    - Virginia Department of Education license (please state your area(s) of licensure)
    - Community of Practice/Informal learning community(s) (Please list)
    - Other (please specify)
1. Have you used the Virginia Cyber Range in any capacity during the 2020 - 2021 academic year? If the response is no, skip questions of how used.

The Cyber Range in this questionnaire refers specifically to the Virginia Cyber Range.

1. Please select all that apply for how you use the cyber range for cybersecurity education and how often. Primary being it is your primary resource for that specific cybersecurity education area, i.e. homework or assessment tool.

Cyber Range Resource	**Class teaching and learning activity**	**Homework activity**	**Assessment tool**	**Professional Development**	**Enrichment/ Other use**
Hands-on laboratory exercise in an immersive environment	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Weekly Workshop Series	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Video lessons	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Capture the Flag (CTF) events	Primary Secondary Barely Not at all	Primary Secondary Barely Not at all	Primary Secondary Barely Not at all	Primary Secondary Barely Not at all	Primary Secondary Barely Not at all

	N/A	N/A	N/A	N/A	N/A
Other Cyber Range Resource	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Community of Practice	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A

1. Please describe how you use the cyber range for enrichment and/or other use and the usage level for cybersecurity education: primary, secondary, or barely.
2. Please provide some specific examples of how you use the cyber range to support your teaching and learning activities.
3. Please provide some specific examples of how you use the cyber range to support your assessment efforts.
4. Please provide some specific examples of how you use the cyber range to provide feedback to your students.
5. Please provide some specific examples of how you use the cyber range for teamwork and collaborative activities.
6. How often do you use the cyber range? (in the last year, how many hours, on average).
7. What percentage of your total cyber range usage do you utilize the following items?

    0. Hands-on Labs (List the three most used)
    1. Weekly Workshop Series
    2. Video Lessons
    3. CTFs
    4. Other cyber range resource (Please list them here)
    5. Community of Practice

2. What percentage of all the resources you utilize to teach cybersecurity education, does the cyber range contribute for the following items?

    0. Class teaching and learning activities
    1. Homework
    2. Assessment tool
    3. Professional development
    4. Enrichment/Other use

2. How do you describe your gender identity? Male, Female, Prefer to self-describe; below:
3. With which racial group(s) do you identify? (Mark all that apply) American Indian or Alaska Native; Hispanic, Latino, or Spanish origin; White; Black or African American; Asian; Middle Eastern or North African; Native Hawaiian or Other Pacific Islander; Another race or ethnicity not listed above:

APPENDIX C
Examples of the Coding Steps

Please provide some specific examples of how you use the cyber range to support your teaching and learning activities.	Summary ideas from the responses
CyberSecurity 02 Ubuntu Linux - Bash Basics CyberSecurity 00 Windows 10 Lab CyberSecurity 01 Kali-Linux Lab Laboratory exercise: Cyber Basics - Introduction to the Linux Terminal and Understanding Directories	Cybersecurity lessons for Linux - Bash Basics, Windows 10, and Kali-Linux to intro to Linux terminal and understanding directories.
- An entire unit on Command Line Interface (Linux) to get familiar with the command line. - Lab and assignments using mcrypt in Linux when teaching about encryption - Lab and assignments using John the Ripper when teaching about hashing/passwords/authentication - Lab using ifconfig, nmap, nslookup, dig, when teaching about Networking Basics - Lab and assignment on Windows password, account lockout and user rights assignment settings when teaching about Data & Network Defense - Lab and assignment in both Linux and Windows when teaching about users, groups, and share permissions in a unit on User Security	Linux environment and tools such as John the Ripper, nmap, nslookup, network defense concepts, users/groups permission settings for User security concepts
In CS 2104 we have three CTF group-based classwork assignments where, for each, students attempt to solve challenges in a specific domain (web reconnaissance, cryptography, networking).	CTF challenges
We use the Cyber Basics environment for the Linux Machine. Additionally, we use the CTF activities for fun additional practice, as well as for demonstrative purposes.	Linux Machine and CTF for practice and demonstration
After each lesson on a technical subject I often assign one of the existing problems in the CloudCTF related to it as a supporting/reinforcing assignment.	Used CTF related problems to the current technical content as a supporting/reinforcing assignment.

Appendix Table B1: Summary Ideas of the Usage of the Cyber Range to Support Cybersecurity Educator Teaching and Learning Activities

Please provide some specific examples of how you use the cyber range to support your teaching and learning activities.	Summary ideas from the responses	Codes from the summary ideas
For example, we have used lessons regarding the understanding and use of the Kali Linux command line this week. Guided exercises that work are engaging to the students--much more than the vocabulary driven work we have in the textbook.	Supports hands-on application of concepts, such as Kali Linux command line practice versus textbook vocab memorization.	hands-on application labs
After each lesson on a technical subject I often assign one of the existing problems in the CloudCTF related to it as a supporting/reinforcing assignment.	Used CTF related problems to the current technical content as a supporting/reinforcing assignment.	labs reinforce lessons CTF
I use the cyber range as a hosting environment for cybersecurity labs and to pull from content. Our textbook (Principles of Cybersecurity) does not currently have a lab manual that is worth using (outdated and no live environment) the cyber range fills that gap.	Use to support textbook content by using the VaCR labs/environment	labs accessible environment

Appendix Table B2: Initial Codes of How Educators Used the VaCR for Their Cybersecurity Teaching and Learning Activities

Hands-on Practice	Existing Labs and Lessons	CTFs	Safe and Accessible Environment
demonstrate learning	Linux	CTFs	VM
hands-on application	Labs for homework	CTF preparation	VM - safe environment
practical application	Lab assignments	CTF - homework	supplemental environment
hands-on practice reinforce learning	Labs reinforce lessons	CTF - group assignments	supplemental environment - supports textbook labs
	Labs aligned with LOs	CTFs, summer camps, and Cyberpatriot - team effort	supplemental environment - support use of third party tools
	Labs - extra credit	CTF - teamwork	supplemental environment - hacking tools
	Outreach support	CTF - team SMEs	Safe sandbox

Appendix Table B3 Themes and their Supporting Codes for How Cyber Ranges are Used for Teaching and Learning Activities

APPENDIX D
Academic Courses Taught by VaCR Registered Educators

High School Courses	Community College Courses	University/College Courses
Accounting, Econ and Personal Finance, & Marketing	CompTIA A+ certification	Breach Remediation
Prob/Stats & Discrete Math	CompTIA Security+ preparation	Computer Networks
AP Physics 1, IB Physics SL, & Physics	Computer Crimes and Hacking	Cyber Forensics
Adv Cybersecurity Software Operations	CSC 200 Intro Comp Sci	Cyber Security II
Adv Cybersecurity Systems Technology	CSC 201 - Computer Science I	Intro to Cybersecurity
Advanced Information Systems	CSC 205 - Computer Organization	Intro to Digital Forensics
Cisco	IT 106 Microcomp OS	Intro to Problem Solving in CS
Computer Network Software Operations	ITD 130 Database Software	Securing the Cyber World
Computer Systems Technology I	ITE 115 Micro Comp Software	Strategic Management
Cybersecurity Fundamentals and Advanced	ITE 130 - Internet Services	Strategy Competition Analytics
Cybersecurity Network Systems	ITE 140 Adv Spreadsheeting	
Cybersecurity Software Operations	ITN 101 Introduction to Network Concepts	
Cybersecurity Systems Technology and Advanced	ITN 170 Linux Sys Admin	
Game Design and Advanced	ITN 171 UNIX	
Hardware and Networking	ITN 200 Administration of Network Resources	
Information Systems	ITN 260 Intro Network Security	
Intro to CS with Python	ITN 275 Incident Response and Computer Forensics	
Introduction to Computer Science	ITN-262: Network Comm, Security & Authentication	
Intro to Programming	ITP 100 Software Design	
IT Fundamentals	ITP 120 Java	
M284 Adv Programming	ITP 270 Programming for Cybersecurity	
M286 Intermed Programming		

M288 AP Computer Science Principles		
Network+		

APPENDIX E
Educator Excerpts Regarding Teaching and Learning Activities Using the VaCR

Accessible Environment	*"We compete in the National Cyber League. Some of the challenges require tools that are installed on Kali Linux, so the VACR Kali image is excellent. Students don't have to download and install Kali. Of those students that have VMware, several do not have enough disk space to have multiple VMs." [Experienced, Community College]* *"I use the cyber range as a hosting environment for cybersecurity labs." [Experienced, High School]*
Hands-on Application & Practice	*"Being able to use the virtual machines online has been amazing. We use them to practice Windows management, which would normally be blocked, learn terminal/command line, and cybersecurity exercises."[Experienced, High School]* *"Use cyber range environments for application of network reconnaissance, footprinting, enumeration principles, firewall and IDS configuration principles, and for public key cryptography concepts." [Experienced, College]*
Existing Labs & Lessons	*"Our textbook does not currently have a lab manual that is worth using (outdated and no live environment) the cyber range fills that gap." [Experienced, High School]* *"Some of the labs provided by the publisher do not directly map to specific learning objectives for the course so I identified more appropriate ones in the range." [Experienced, College]*
CTFs	*"After each lesson on a technical subject I often assign one of the existing problems in the CloudCTF related to it as a supporting/reinforcing assignment." [Experienced, High School]* *"We have three CTF group-based classwork assignments where, for each, students attempt to solve challenges in a specific domain (web reconnaissance, cryptography, networking). [Experienced, College]*

APPENDIX F
Educator Excerpts Regarding Feedback and Assessments Using the VaCR

Formative Assessment	*"Using the cyber range gives students the opportunity to ask questions about something they maybe didn't fully grasp before." [Novice, High School]* *"I use the labs given via the range or cyber.org to help them better understand where their weaknesses are and what they need to improve on." [Experience, Community College]*
Summative Assessment	*"Assessments are based on successful completion of tasks assigned directly relating back to course competencies." [Novice, High School]* *"I sometimes write CTF problems as "quiz" problems, which serve as self-grading activities." [Experienced, High School]*
Feedback	*"I ask my students if they like the labs and what their favorite part is." [Novice, High School]* *"Students will be assigned specific tasks, most recently account management policy via Windows Local Security Policy. Each student needed to properly configure the settings, as outlined in the assessment. I logged into each machine to verify settings and give feedback." [Experienced, Community College]*