Issues in Information Systems
Volume 23, Issue 3, pp. 128-138, 2022

DOI: https://doi.org/10.48009/3_iis_2022_111

The role of cyber competitions in cyber defense education: A case study of National Cyber League (NCL) participation

Ping Wang, *Robert Morris University, wangp@rmu.edu*
Hubert D'Cruze, *University of Maryland, hubert.dcruze@yahoo.com*

Abstract

This research paper explores the value of cybersecurity competitions in cyber defense education and its impact on the cybersecurity industry and workforce development. Competitions are considered active and challenge based learning that can be used as effective pedagogies to improve student interest, motivation, and problem solving in education. For cyber defense education quality assurance, student participation in cyber competitions is required for the National Centers of Academic Excellence in Cyber Defense Education (NCAE-CDE) designation by the US National Security Agency and Department of Homeland Security (NSA/DHS). This research is based on the Challenge Based Learning (CBL) framework and explores the pedagogical benefits of cybersecurity competitions through the case study of the National Cyber League (NCL) competition. The case study in this research focuses on mapping the features and knowledge and skill domains of the NCL competition to relevant NCAE-CDE program criteria and knowledge units and presents sample data on students' participation and performance from a NCAE-CDE designated institution. This study also analyzes the quantitative data and qualitative observations and reflections on student participation in the NCL competition and their performance in cyber defense educational programs.

Keywords: Challenged based learning, CBL, cyber competition, cyber defense education, NCAE-CDE, CAE-CD, National Cyber League, NCL, knowledge units

Disclaimer: This research paper only represents the personal opinions of the authors and does not in any way represent any official positions of any affiliated institution or government agency.

Introduction

Cybersecurity education research is of increasing interest and significance as educational and training programs in Cybersecurity have been on the rise due to increasing workforce demand. There has been a substantial and growing workforce demand for better trained and qualified cybersecurity professionals to defend our cyber space and critical assets against various cyber threats and attacks (U.S. Department of Labor BLS, 2022; Wang & Sbeit, 2020). Meanwhile, the cybersecurity workforce gap persists as a result of inadequate supply of qualified cybersecurity professionals for the growing demand in North America and around the world. The latest cybersecurity workforce survey study conducted by the non-profit (ISC)^2, the International Information System Security Certification Consortium, shows that the annual cybersecurity workforce gap or shortage is approximately 2.7 million around the world and over 400,000 in North America and that two-thirds of the study participants have reported concerns of security risks for their organizations due to a cybersecurity staffing shortage ((ISC)^2, 2021). The study also shows the trend that the cybersecurity workforce gap is increasing in North America, Europe and Latin America while it is decreasing in Asia-Pacific countries ((ISC)^2, 2021). Therefore, it is a significant practical and research issue for cybersecurity educators and researchers to seek effective teaching and learning activities to motivate cyber students and develop adequate and qualified cyber talent for the workforce.

Cybersecurity is a rewarding but challenging professional field, which demands quality education and training for students to acquire both technical and non-technical knowledge, skills, and abilities to contribute effectively to a diverse multi-disciplinary cybersecurity work team in the future (Blair, Hall, & Sobiesk, 2019). Cyber defense competitions have been used by educators as an active learning activity to stimulate student interest in cybersecurity education and careers and improve their technical knowledge and hands-on skills and non-technical skills such as problem solving, critical thinking, teamwork, leadership, and communication skills (Conklin, 2006; De Zan, 2022; Joyce, Day, & Evans, 2018; La Fleur, Hoffman, Gibson, & Buchler, 2021; Sener, 2016). However, there has been little research on assessing the quality and effectiveness of integrating specific cyber competitions with cybersecurity education outcomes using standard metrics.

Quality assurance is the key to effective teaching and learning and successful preparation of qualified workforce. Given the fast growth of cybersecurity programs, a credible quality assurance system is necessary to evaluate program outcomes and sustain the quality and reputation of cybersecurity education and training programs and providers. In the United States, the National Centers of Academic Excellence in Cyber Defense Education (NCAE-CDE) designation program jointly sponsored by the National Security Agency (NSA) and Department of Homeland Security (DHS) has been the most comprehensive and reputable national standard for evaluating and certifying cybersecurity education programs with comprehensive and measurable program criteria and specific knowledge units and learning outcomes for assessment (Wang, Dawson, & Williams, 2018). Documentation and evidence of student participation in and faculty support for cyber competitions are required for the respective Students and Faculty criteria in the Designation Requirements and Application Process for NCAE-CDE designation (APAR, 2022).

There are a variety of local, regional, and national cyber defense competitions for students in the United States with various content design and participation rules. This research is to focus on the case of the National Cyber League (NCL) competition, which is a virtual and flexible cyber competition open to all students in colleges and high schools with large numbers of student participation each season. The goal of this study is to identify the features of the NCL competition and analyze the learning effectiveness of sample student participation from the perspective of the challenge based learning (CBL) theory. The study will present a CBL-based analytical model with metrics for assessing the value of cyber competitions and contribute empirical data of student participation and learning to the field of cybersecurity education. The following sections of the paper present the relevant background, the NCL case study, quantitative and qualitative data of sample student participation in the NCL competition from multiple seasons, as well as discussions of the data and conclusions.

Background

Cybersecurity competitions, or cyber competitions for short, can be used as extra-curricular activities for students or embedded in course or curricular activities. Educators and researchers have observed that cyber competitions may bring multiple benefits to student learning and positive impacts on key aspects of cybersecurity education. Sener (2016) has identified the following benefits of cyber competitions as event-anchored learning: (1) Cyber competitions provide students valuable learning experience for them to practice, apply, and develop technical skills and non-technical skills such as problem solving, time management, teamwork and communication skills; (2) Cyber competitions are fun and motivating experience that helps student participants to increase their interest and motivation in cybersecurity education and careers; (3) Cyber competitions integrate practical hands-on learning with theory-based learning in traditional classrooms; (4) Cyber competitions may provide additional professional networking opportunities to identify and develop cybersecurity employers and employment opportunities for cyber talent. Beyond these direct learning benefits for students, cyber competitions may have wider positive impacts on other key aspects of the cybersecurity education environment, including student and program development, curriculum improvement, faculty professional development, and student career development (Sener, 2016). Cyber competitions may be used for broader educational and social impacts. For example, cyber competitions are useful activities for building and maintaining partnerships between 2-year community colleges and 4-year institutions to create more educational and professional opportunities for community college students (Rursch & Jacobson, 2009). In addition, cyber competitions such as the Capture-the-Flag (CTF) can be used as an effective gamification approach in learning to develop and improve student interest in cybersecurity among under-represented minority student populations (Kornegay, Arafin, & Kornegay, 2021).

Cyber defense competitions provide primary opportunities for students to be engaged in an active learning process with interactive hands-on activities and experience and collaborative learning through team building and team skill development activities (Conklin, 2006). In the light of individual constructivism and social constructivism, active learning strategies and activities promote higher levels of student engagement to encourage students to interact cognitively, socially, and behaviorally with the educational content and processes for individual and collaborative knowledge construction (Jiwani, 2015). Results of experimental research using a competitive active learning platform indicate that competitive active learning has a significant positive impact on student attitude and motivation, student engagement, critical thinking, and academic performance (Kapoor, Hua, & Anastasiu, 2018). Competitive behavior involving social comparison, reward, and competition can be powerful intrinsic persuasive strategies used to motivate learners toward successful outcomes in education (Orji, Greer, & Vassileva, 2019). Pedagogically, active learning requires learner-centeredness, focus on process and content, interdisciplinary and collaborative lessons, and focus on student self-motivation and reflection; the specific pedagogical strategies of active learning may include problem-based learning, discovery-based learning, inquiry-based learning, project-based learning, and case-based learning (Cantaneo, 2017).

Challenge Based Learning (CBL) is a type of active learning that is applicable to cybersecurity education. CBL has been widely used in higher education and typically involves active learning techniques of problem-based learning, project-based learning, and inquiry-based learning to improve student engagement and performance (Leijon, Gudmundsson, Staaf, & Christersson, 2021). The CBL methodology has been applied to cybersecurity competitions for students to apply their knowledge and skills for problem-solving in the learning process (Cheung, Cohen, Lo, & Elia, 2011). Challenge Based Learning (CBL) is a learning framework originated from the Apple Classrooms of Tomorrow – Today (ACOT^2) project initiated in 2008, and the goal of the framework is to empower learners to address real-world challenges while acquiring multi-disciplinary knowledge and skills necessary to be a productive member of the society (Nichols, Cator, & Torres, 2016). According to the CBL framework, Challenge Based learning should have the following characteristics and metrics:

1. A flexible and customizable framework as a guiding pedagogy or integrated with other approaches for implementation.
2. A scalable model with multiple points of entry.
3. A free and open system free from proprietary ideas, products, or subscriptions.
4. A learner-centered process that emphasizes learners' direction and responsibilities in learning.
5. An authentic environment that integrates academic standards with content.

6. A focus on global ideas and challenges with localized solutions that are appropriated for all age groups.
7. A real connection between academic disciplines and real-world experience.
8. A framework to develop 21st century (future) skills.
9. Purposeful use of technology for research, analysis, organization, collaboration, networking, communication, publication, and reflection.
10. The opportunity to empower learners to make a difference.
11. A method to document and assess the learning process and products.
12. An environment for in-depth reflection on teaching and learning.
(Nichols, Cator, & Torres, 2016).

The CBL framework consists of three interconnected and progressive phases:

1. Phase 1 – Engage: Learners explore big ideas as broad concepts, contextualize and personalize the concepts through essential questioning to turn the abstract big idea into a concrete and actionable challenge.
2. Phase 2 – Investigate: Learners participate in the guiding activities and learning the knowledge and resources necessary to build the foundation to identify solutions to address the challenge.
3. Phase 3 – Act: Learners develop evidence-based solutions to the challenge, implement the solution, and assess the effectiveness of the solution based on the results.

There are various local, regional, national cyber competitions that are sponsored by various organizations. This research will focus on the study of the National Cyber League (NCL) competition with sample student participation using the Challenge Based Learning framework and NCAE-CDE program criteria.

Case Study: NCL

The National Cyber League (NCL) is a biannual, seasonal, and all-virtual competition founded in 2011 with the mission "to prepare the next generation of cybersecurity professionals by providing high school and college students, as well as their coaches, an online, safe platform of real-world cybersecurity challenges" with more than 13,000 students from over 650 colleges and high schools across all 50 states of the U.S. participating each year (NCL, 2022). Each NCL season activities consist of open gym, practice game, individual game, and team game. The spring and fall season calendars of NCL each year fit with most regular college and school semesters, which makes it easy for aligning NCL activities to student course work during each semester.

NCL activities are conducted totally online via web browser using NCL cloud-based servers, which are easily accessible to any registered student anywhere with Internet connection. This is a strength to make the competition activities more scalable, accessible, and affordable. Most existing cyber competitions are in-person, which require costly investments in hardware labs and travel for participation resulting in less access and participation. The all-virtual activities of NCL competitions utilize virtualization technology which "enables the creation and deployment of computer security lab exercises while minimizing the associated configuration time and the associated hardware requirements" (Manson & Carlin, 2011, p.6). As a result, NCL seasons are more scalable, accessible, and affordable with a minimal registration cost of $35 per season registration and no cost for travel. The NCL season activities may also be used by faculty coaches as part of the course work for credit. Therefore, the virtual NCL competition platform has the key metrics 1 and 2 of the Challenge Based Learning (CBL) framework as a flexible, customizable, and scalable model as well as metrics 9 of CBL for its purposeful use of the virtualization technology and NCL cloud services for research, analysis, organization, collaboration, and communication on the cyber game activities.

NCL competition activities also reflect the three progressive phases of the Challenge Based Learning (CBL) framework: Engage, Investigate, and Act. Students in NCL competitions participate in the Capture-the-Flag (CTF) security challenge game. Here is NCL's description and expectation for the CTF game process:

> In CTF games, players race to solve security-related challenges, often searching for digital 'flags' hidden on servers, in encrypted text, or in applications. Challenges within the CTF are open-ended and require expertise and skills in a wide range of security-related topics: computer forensics, cryptography, network penetration testing, web security, system or network administration, etc. When a player submits a flag (or correct answer), they receive points for solving the challenge. The player or team with the highest cumulative score at the end of the game wins.
> (NCL FAQ, 2022).

The virtual and asynchronous design of the NCL game allows students to digest and internalize the challenge and questions, research and investigate possible solutions using their knowledge, skills and resources, and reach a final solution as answer to the challenge. The NCL challenge activities using CTF games reflect metrics 3, 4, 5, and 10 of the CBL framework: A free and open system for open-ended exploration, a learner-centered process where the students are empowered to takes control of the learning process to address the challenge. Given that NCL student participants include all age groups from all states in the U.S. and that the challenge questions are related to security issues that exist around the world, the NCL competition also reflects metric 6 of the CBL framework on global challenges with localized solutions for all age groups.

NCL's mission to prepare the next generation cybersecurity workforce and its focused practice of applying school learning to real-world challenges reflects more metrics of the CBL framework, including metrics 7 and 8 on bridging academic disciplines and real-world experience and developing 21st century skills. The detailed performance and assessment reports and communication forums for student players and for faculty coaches reflect metrics 11 and 12 on documentation and assessment of the learning process and on reflection of teaching and learning.

As more specific evidence of bridging academic learning to real world challenges for workforce preparation, the knowledge and skills domains and categories of NCL cyber competition questions and challenges are mapped to the widely used Cybersecurity Work Roles created and published by the National Initiative for Cybersecurity Education (NICE) under NIST (National Institute of Standards and Technology (NICE, 2020). The NCL exercise and game challenges and questions include the following 9 domains and categories, which reflect up-to-date real-world cybersecurity challenge areas (NCL FAQ, 2022). The detailed mapping to NICE framework work roles is posted at NCL website.

- **Open Source Intelligence:** Utilize publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.
- **Cryptography:** Identify techniques used to encrypt or obfuscate messages, and leverage tools to extract the plain text.
- **Password Cracking:** Identify types of password hashes and apply various techniques to efficiently determine plain text passwords.
- **Log Analysis:** Utilize the proper tools and techniques to establish a baseline for normal operation and identify malicious activities using log files from various services.
- **Network Traffic Analysis:** Identify malicious and benign network traffic to demonstrate an understanding of potential security breaches.

- **Forensics:** Utilize the proper tools and techniques to analyze, process, recover, and/or investigate digital evidence in a computer-related incident.
- **Scanning:** Identify and use the proper tools to gain intelligence about a target including its services and potential vulnerabilities.
- **Web Application Exploitation:** Identify actionable exploits and vulnerabilities and use them to bypass the security measures in online services.
- **Enumeration and Exploitation:** Identify actionable exploits and vulnerabilities and use them to bypass the security measures in code and compiled binaries.

These NCL knowledge and skills domains and categories are also mapped to the exam question domains of the vendor-neutral and industry-recognized Security+ certification provided by CompTIA (Computing Technology Industry Association) to validate learners' cybersecurity qualifications (NCL, 2022).
In addition, the NCL knowledge and skills domains and categories are mapped to the program criteria and knowledge units (KUs) for NSA Centers of Academic Excellence in Cyber Defense (CAE-CD) designation to support quality assurance in cybersecurity education. Documented evidence of student participation and faculty support for cyber competitions including NCL are respective requirements for the Students and Faculty criteria to apply for CAE-CD designation and redesignation (APAR, 2022). CAE-CD designation and redesignation also require specific documentation and artifacts of various numbers and combinations of knowledge units (KUs) in the cybersecurity program of study (PoS) for designation based on an associate, bachelor's, master's, or doctoral program (APAR, 2022). NCL challenge activities embedded in teaching and learning can be used as documentation of KUs because NCL has aligned its knowledge and skills domains and categories to specific CAE-CD KUs and learning outcomes. Table 1 below is a summary of NCL challenge domains mapped to CAE-CD KUs (NCL, 2022).

Table 1: NCL Domains Mapped to CAE-CD Knowledge Units

NCL Skills Domains/Categories	CAE-CD Knowledge Units
Open Source Intelligence	Cyber Threats (CTH)
Cryptography	Basic Cryptography (BCY), Advanced Cryptography (ACR)
Log Analysis	Basic Scripting and Programming (BSP), Fraud Prevention and Management
Network Traffic Analysis	Basic Networking (BNW), Network Defense (NDF), Advanced Network Technology and Protocols (ANT), Intrusion Detection/Prevention Systems (IDS), Network Forensics (NWF), Network Technology and Protocols (NTP)
Forensics	Device Forensics (DVF), Digital Forensics (DFS), Host Forensics (HOF), Media Forensics (MEF)
Web Application Exploitation	Databases (DAT), Database Management Systems (DMS), Web Application Security (WAS)
Scanning & Reconnaissance	Cloud Computing (CCO), IA Architectures (IAA), Operating Systems Hardening (OSH), Vulnerability Analysis (VLA)
Enumeration & Exploitation	Operating System Concepts (OSC), Algorithms (ALG), Advanced Algorithms (AAL), Data Structures (DST), Industrial Control Systems

	(ICS), Linux System Administration (LSA), Operating Systems Administration (OSA), Windows System Administration (WSA), Low Level Programming (LLP), Secure Programming Practices (SPP), Software Reverse Engineering (SRE), Software Security Analysis (SSA), Penetration Testing (PTT)

The alignment of NCL skills domains and categories to specific knowledge units and learning outcomes for CAE-CD designation helps students to integrate their academic learning at CAE programs with their hands-on practice and problem-solving and learning on real-world challenges on the NCL platform. The alignment to CAE-CD KUs enables faculty coaches to embed NCL activities and performance in curricular and course activities and assessment. The mapping between NCL skills domains and CAE-CD KUs and outcomes also allows student learning experience with NCL competitions to be used as documented evidence and artifacts for quality assurance and for CAE-CD designation and redesignation applications.

Findings and Discussions

This section presents and discusses the quantitative and qualitative data on student participations in the NCL competitions from a private non-profit university in northeastern United States, which has an active CAE-CD designation from NSA/DHS in good standing. The NCL student participations were for eight seasons during the past four academic years from the fall 2018 season to the spring 2022 season. The NCL participation was offered as an optional opportunity to both undergraduate and graduate students in several courses in the BS Cybersecurity and MS Cybersecurity programs at this university. This research only presents the data for the undergraduate participants in NCL, which are the majority of the participation during the 8 seasons. To respect the students' role in the learning process, the NCL participation was not required but optional and voluntary with faculty guidance and the incentive of substitution credit for the final exam or project as encouragement from the faculty member. The incentive was well justified because the student participants put in extensive hard work for NCL during the semester to complete the season and have to submit their detailed completion report from NCL for assessment on their performance on each knowledge and skill domain. The courses for the undergraduate participants for this study are: Networks and Data Communication, Computer Network Security, and Ethical Hacking/Advanced Topics in Cyber Defense. The NCL challenge domains and topics are integrated with many topics of these courses, which enable students to apply their classroom learning to the NCL challenges and to reinforce their coursework with their NCL participation experience. Table 2 below summarizes the common knowledge and skills areas and major learning outcomes shared between these courses and the NCL domains.

Table 2: Shared Domains and Outcomes between Coursework and NCL

Courses	NCL Domains	Sample Shared Learning Outcomes
Networks & Data Communication	Network Traffic Analysis	Identify components of the OSI model; Trace network packet captures and data flow; Use tools for scanning and packet analysis; Identify network typography and design; Identify network security vulnerabilities; Analyze network layers and protocols; Interpret network traffic to determine security practices.

Computer Network Security	Network Traffic Analysis;
	Cryptography;
	Open Source Intelligence
		Examine network traffic to identify attacks and threats;
		Scan for vulnerabilities using common tools;
		Identify cryptographic schemes and use cases;

		Describe strengths/weaknesses of encryption solutions; Identify general software vulnerabilities and CVEs; Identify properties of SSL, VPN, hashing, PKI.

Ethical Hacking & Advanced Topics in Cyber Defense	Log Analysis;
	Network Traffic Analysis;
	Web Application & Exploitation;
	Scanning & Reconnaissance;
	Enumeration & Exploitation
		Use scripting languages to analyze log files;
		Identify the elements of a fraudulent transactions;
		Analyze network traffic to identify intrusion attempts;
		Identify web security flaws and exploitations;
		Identify ICS protocols and applications;
		Scan operating systems for security vulnerabilities;
		Identify threats and attacks against cloud services;
		Examine software source code to identify security issues;
		Demonstrate basic proficiency of command line capabilities
		Manager users, passwords, and security policies;
		Audit security logs;
		Perform penetration testing to identify application security flaws and vulnerabilities.

Table 3: Student Participation in NCL & Course Performance

NCL Season	NCL Participants (N)	NCL Domains Completion (AVG)	Participant Course Success Rate (AVG)	Overall Course Success Rate (AVG)
Spring 2022	6	79.9%	93.7%	88.4%
Fall 2021	8	75.8%	90.5%	86.1%
Spring 2021	4	81.3%	96.8%	91.2%
Fall 2020	7	73.5%	89.4%	85.3%
Spring 2020	6	61.8%	87.6%	86.8%
Fall 2019	6	65.4%	88.7%	84.6%
Spring 2019	4	57.6%	83.1%	85.7%
Fall 2018	1	66.5%	100%	87.1%

Table 3 above presents the quantitative summary findings of the sample students' participations in each NCL season from Fall 2018 through Spring 2022. The table shows the total number (N) of voluntary undergraduate student participants at the private university for this study, the average completion rate of the NCL skills domains, the average success rate of these participants in the 3 courses mapped in Table 2, compared to the overall average class success rate in the participating courses. The NCL domains completion rate is based on all the activities they have participated on the NCL platform during the season, including the Gymnasium for practice and training, Practice Game, Individual Game, and Team Game. The course success rate is defined as achieving 70% or higher for these undergraduate courses. This study uses the activity completion rate without the actual scores for each activity because the study emphasizes and focuses on the value of student participation and experience with NCL activities and challenges.

The summary findings show a general increase in the average NCL domain completion rate. The participation and completion of NCL domains appear to help the student participants with their course work at the sampled university as higher average completion rates occur with higher average course success rates in this dataset most of the time. In addition, The NCL student participants' average course success rates appear to be higher than the average overall course success rates in the participating classes. Of course, this is only a preliminary study on this subject with limited participants and data.

Some student participants also provided qualitative reflections and comments on their NCL experience to the faculty coach. The following are some excerpts of the student reflections and comments:

- "I had a lot of fun with NCL and will probably enroll again in the spring."
- "I really enjoyed participating in the NCL competition and am even considering doing it again."
- "This competition was an excellent opportunity to learn new skills. Our team have decided to participate again next season."
- "I have competed the Cyber Skyline [NCL] competition and would like to first, thank you for this opportunity! I found these challenges to be quite hard but this was also a really fun experience in trying to complete some of the harder topics."
- "I truly enjoyed the game and will most likely participate again in the future. I think it is a great way to test my skills and see how they improve as I progress in my education. Thank you for the opportunity!"

The qualitative reflections and comments from the student participants indicate that the students truly enjoyed the NCL competition activities, which stimulated their interest in participation and desire to continue their participation in the future. Secondly, some students do feel that the NCL game activities are not easy but challenging, but at the same time they feel they are learning something. This is important feedback to show that students are aware of their learning process of facing challenges and addressing challenges with their knowledge and skills.

Conclusions

Cyber competitions are considered challenge based active learning activities, which are required for CAE-CD designation and re-designation by NSA/DHS for cybersecurity education quality assurance. This study analyzes cyber competitions using the metrics of the Challenge Based Learning (CBL) framework with a focused case study on the National Cyber League (NCL) competition and NCL participations from students in a private U.S. university for 8 seasons. The 9 challenge and skill domains of NCL are mapped to cybersecurity work roles of the NIST NICE workforce framework and vendor neutral Security+ certification exam question domains. The NCL activity domains and categories are also mapped to specific knowledge units (KUs) required for the CAE-CD designation as well as certain coursework at the sample CAE institution. The sample student participation data and reflections suggest that the NCL participation experience may help with student coursework in cybersecurity mapped to the NCL domains. The following is a summary of the conclusions of this study:

- NCL domains are well mapped to key NCAE-CD designation criteria and KUs.
- NCL domains can be mapped to specific cybersecurity courses and learning outcomes.
- NCL completion rates appear to correlate with success rates in courses mapped to NCL domains.
- NCL participation experience may help with student coursework mapped to NCL domains.
- Students enjoy the experience and recognize value of learning in participating in NCL.

However, this is a only preliminary study with limited data and observations. Future studies may include more student participants for wider analysis. Future studies may also focus on specific challenge questions in NCL and their direct impact on a course learning outcome if it is possible to have NCL disclose the questions. Other possible areas for further research may include exploring the impact of NCL participation on student critical thinking and problem solving skills and career development as well as comparing the pedagogical impact of NCL with other cyber competitions.

References

(ISC)^2. (2021). A resilient cybersecurity profession charts the path forward: (ISC)^2 cybersecurity workforce study 2021. Retrieved from https://www.isc2.org/Research/Workforce-Study

APAR (Application Process and Adjudication Rubric), Cyber Defense Working Group (CDWG). (2022, May). National Centers of Academic Excellence in Cybersecurity CAE 2022 Designation Requirements and Application Process for CAE-Cyber Defense (CAE-CD). Retrieved from https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass_cae-cyber-defense-program-guidance.pdf

Blair, J.R.S., Hall, A.O., & Sobiesk, E. (2019). Educating future multidisciplinary cybersecurity teams. *Computer,* March 2019. 58-66.

Cantaneo, K.H. (2017). Telling active learning pedagogies apart: From theory to practice. *Journal of New Approaches in Educational Research, 6*(2). 144-152.

Cheung, R.S., Cohen, J.P., Lo, H.Z., & Elia, F. (2011). Challenge Based Learning in cybersecurity education. Retrieved from https://josephpcohen.com/papers/cbl.pdf

Conklin, A. (2006). "Cyber defense competitions and information security education: An active learning solution for a capstone course. *Proceedings of the 39th Hawaii International Conference on System Sciences – 2006.* 1-6.

De Zan, T. (2022). Mitigating the cyber security skills shortage: The influence of national skills competitions on cyber security interest (Doctoral Dissertation). University of Oxford, UK.

Jiwani, F. (2015). Exploring the theory of constructivism through active learning strategies in a classroom. *Third 21st CAF Conference at Harvard, in Boston, USA. September 2015, 6*(1). 135-144.

Joyce, A., Day, S., & Evans, N. (2018). Educational competitions to boost the cyber workforce development. *Proceedings of 2018 National Cyber Summit Research Track.* DOI 10.1109/NCS.2018.00010

Kapoor, M., Hua, S., & Anastasiu, D.C. (2018). Improving student motivation through competitive active learning. *Proceedings of 2018 IEEE Frontiers in Education Conference (FIE)*. 1-5.

Kornegay, M.A., Arafin, M.T., & Kornegay, K. (2021, July). Engaging underrepresented students in cybersecurity using Capture-the-Flag (CTF) competitions (experience). *2021 ASEE Annual Conference.* Paper ID #33091. 1-6.

La Fleur, C., Hoffman, B., Gibson, C.B., & Buchler, N. (2021). Team performance in a series of regional and national US cybersecurity defense competitions: Generalizable effects of training and functional role specialization. *Computers & Security, 104* (2021 102229. 1-18.

Leijon, M., Gudmundsson, P., Staaf, P., & Christersson, C. (2021). Challenge based learning in higher education: A systematic literature review. *Innovations in Education and Teaching International.* 1-10. DOI: 10.1080/14703297.2021.1892503.

NCL. (2022). The National Cyber League. Retrieved from https://nationalcyberleague.org/

NCL FAQ. (2022). Frequently Asked Questions. Retrieved from https://nationalcyberleague.org/faq

NICE (National Initiative for Cybersecurity Education), NIST (National Institute of Standards and Technology. (2020). NICE Cybersecurity Workforce Framework (SP800-181 Revision 1). Retrieved from https://doi.org/10.6028/NIST.SP.800-181r1

Nichols, M., Cator, K., & Torres, M. (2016). *Challenge based learner user guide.* Redwood City, CA: Digital Promise.

Orji, F.A., Oyibo, K., Greer, J., & Vassileva, J. (2019). Drivers of competitive behavior in persuasive technology in education. *Adaptive and Personalized Persuasive Technology (ADAPPT 2019) Workshop, UMAP'19 Adjunct, June 9–12, 2019, Larnaca, Cyprus.* 127-134.

Rursch, J.A., & Jacobson, D. (2009). Using cyber defense competitions to build bridges between community colleges and four year institutions: a footbridge for students into an IT program. *39th ASEE/IEEE Frontiers in Education Conference, October 18 - 21, 2009, San Antonio, TX.* 1-6.

Sener, J. (2016, April). The role of student competitions in cybersecurity education. National Cyberwatch Center. Retrieved from https://www.nationalcyberwatch.org/resource/role-student-competitions-cybersecurity-education/

U.S. Department of Labor BLS (Bureau of Labor Statistics). (2022, May 22). Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Wang, P., Dawson, M., & Williams, K.L. (2018). Improving cyber defense education through national standard alignment: Case studies. International Journal of Hyperconnectivity and Internet of Things. 2(1), 12-28.

Wang, P., & Sbeit, R. (2020). A comprehensive mentoring model for cybersecurity education. In S. Latifi (Eds.), *Advances in Intelligent Systems and Computing* (17-23). Springer Nature Switzerland AG.