ASEE'S VIRTUAL CONFERENCE

At Home with Engineering Education

JUNE 22 - 26, 2020 #ASEEVC

Paper ID #28239

Assessment of Cybersecurity Competition Teams as Experiential Education Exercises

Dr. Jeremy Straub, North Dakota State University

Jeremy Straub is the Associate Director of the NDSU Institute for Cyber Security Education and Research and an Assistant Professor in the Department of Computer Science at the North Dakota State University. He holds a Ph.D. in Scientific Computing, an M.S. and an M.B.A. and has published over 40 journal articles and over 120 full conference papers, in addition to making numerous other conference presentations. Straub's research spans the gauntlet between technology, commercialization and technology policy. In particular, his research has recently focused on cybersecurity topics including intrusion detection and forensics, robotic command and control, aerospace command and 3D printing quality assurance. Straub is a member of Sigma Xi, the AAAS, the AIAA and several other technical societies, he has also served as a track or session chair for numerous conferences.

Assessment of Cybersecurity Competition Teams as Experiential Education Exercises

Abstract

This research paper presents initial work on characterizing the educational value of cybersecurity competition teams to their student participants. It discusses the different types of cybersecurity competitions and provides examples of college student-targeted competitions of each type. The value of these team activities is considered and student outcomes from them are discussed. The paper presents a discussion of ongoing activities to assess the value of cybersecurity team participation.

1. Introduction

This research paper considers the educational value of cybersecurity competition teams to their student participants. There several types of cybersecurity competitions including red team / blue team events, blue team events and capture the flag style events. In the first (red team / blue team) teams attack (red team) and defend against (blue team) the other team's attacks in a direct team-to-team conflict environment. Blue team only events, such as the Collegiate Cyber Defense Competition [1], focus on preparing students to secure networks by using area security volunteers as the attackers with competitors focusing on keeping their systems, servers and network operational the longest. Finally, capture the flag events focus more on the attack side, but also generally involve problem solving. Examples of capture the flag events include the National Cyber League [2], the National Cyber Summit's Cyber Cup [3] and the MITRE Corporation's capture the flag event [4].

This paper presents initial work towards assessing, quantitatively, the benefits enjoyed by students that participate on these teams. Each type of competition requires a different (albeit somewhat overlapping) skillset. As these competitions are available worldwide and can be participated in online, there are ample opportunities for involvement. It is also clear that they all have some relevance to skills that are valuable in the real world; however, the exact level of direct relevance varies by competition type and individual competitions' design.

Participants gain educational value and learn from several sources. Their local-level training and preparation is a key source of learning. In some cases, competitions provide pre-competition training. The National Cyber League, for example, has a 'gymnasium' that is open prior to the competition and walks players through how to solve various types of problems. Participants also learn while they are competing by having to solve problems in a high-pressure situation.

In addition to gaining core technical skills, participants also benefit in other areas. They build teamwork skills in team competitions such as the MITRE capture the flag, the team-based Collegiate Cyber Defense Competition and the team portion of the National Cyber League. Students also gain experience and learn how to work well under pressure (critical for anyone in cybersecurity) and they gain leadership skills. Students who serve as team leaders also learn project management and communications skills.

To assess the efficacy of these competitions, a survey is proposed to collect demographic data, details related to why students opt to participate and the benefits that they sought and attained via their participation. Additionally, the survey seeks to characterize their pre- and post-participation status with regards to several key metrics. Students will also be asked to indicate to what extent they attributed the gains that they reported to program participation. Questions are also planned regarding activities that students participated in and the outcomes achieved. This data will be analyzed to identify contest and benefit correlation and demographic characteristics and benefit correlation.

The paper discusses the value of contest participation and then presents planned future work. This includes a larger scale study and longitudinal tracking of current participants.

2. Background

Cybersecurity competitions are a form of experiential education where student competitors (in the case of student competitions – there are also competitions for the general public) solve puzzles and simulated real-world challenges. The competitions build on a significant body of work related to experiential education and problem-based learning. Each of these topics is now discussed.

2.1. Experiential Education

Experiential education has a long history tracing back to apprenticeships [5]. It has been shown to be beneficial across a wide range of academic levels [6]–[11] and across numerous disciplines [12]–[16]. In addition to its technical benefits, it has also been shown to teach students soft skills [17], improve both creativity [18] and self-image [19] and even increase students' likelihood of securing employment [20].

While the basic concept of experiential education would appear to pre-date the formal study of educational methods, a number of frameworks for facilitating and assessing experiential education techniques have been proposed. Coffield, et al. identified over 70 [21], [22]; however, Kayes suggests that Kolb's model is one of the most widely used [22], [23].

Kolb's model is based on six suppositions. These include: that learning should be considered to be a process (not outcomes), that it is experience-grounded, that it involves concept conflict resolution, that it necessitates holistic adaptation, that it "results from synergistic transactions" between a learner and the learning environment and that it is a knowledge creation process [22]. Kolb's model draws heavily upon the concept of learning styles and several of the forgoing suppositions have elements of learning style doctrine within them. According to Healey and Jenkins [24], learning styles reflect a diversity of environmental considerations including those attributable to gender and cultural differences. Willingham, et al. [25] and others [26]–[28], however, contend that there are inherent problems with the learning styles theories and that they lack scientific rigor.

Kolb's model suggests that experiential learning can be characterized as a four-phase cyclic model. Under this model, learners (1) have an experience, (2) reflect on the experience, (3) conceptualize what they have experienced into a model or theory and (4) plan how to test their model or theory through experience [24].

2.2. Cybersecurity Competitions and Problem Based Learning

Cybersecurity competitions use a type of experiential education commonly called problem-based learning or challenge-based learning. Many competitions (e.g., [29]) are highly aligned with workforce roles, as validated by those currently working in these roles. Competitions have been shown to increase student interest in cybersecurity [30]. They have been shown to be particularly effective for increasing the interest of female students in cybersecurity [30]. They are seen to be an excellent way to broaden participation in cybersecurity education (and eventually cybersecurity careers) by underserved populations [31], [32]. Problematically, at least some competitions have been found to not be gender-inclusive [33].

Competitions have been used for student education within the United States [34] and abroad [35]. Participants typically have "investigative, social, and creative" characteristics [36]. Those with high levels of self-efficacy have been reported [37] to, generally, have positive experiences. Participants with higher cybersecurity skill self-confidence [37], self-efficacy [38], "investigative interests" [38] and a "rational decision making style" [38] tended to report greater interest in pursuing a cybersecurity career after competition completion.

Competition-style activities [39] and competition participation have been included in courses. Despite this, educational outcomes from competitions vary widely and have not been well-defined [40], [41]. Woszczynski and Green have worked towards solving this issue through the identification of key competition learning outcomes [40]. Problematically, cybersecurity competitions have not been shown to produce "more high quality professionals" [42] and Bashir, et al. note that "there has been little empirical evidence of … effectiveness" [43] to-date. While Hoag notes that "there is no obvious connection between team academic characteristics and the outcome of the competition" [44], the competitions have been demonstrated to "pique students' interest" [42]. There has even been a suggestion of adding commentary to increase viewers' excitement [45].

3. Cybersecurity Competition Types

This section provides an overview of several types of cybersecurity competitions. First, red team events are discussed; then, blue team events are presented. Next, red versus blue style and capture the flag competitions are each reviewed. Finally, knowledge competitions and tabletop exercises are summarized.

Red Team / Penetration Testing Events – Red team and penetration testing events place students in the role of penetration testers or ethical hackers. These types of competitions typically involve identifying security vulnerabilities in information technology systems to exploit and exploiting them to gain access to computing resources. Typically, a documentation component is also included where teams report on the security vulnerabilities that they've discovered. An example of a red team event is the Collegiate Penetration Testing Competition [46], which is discussed below.

Blue Team Events – Blue team events focus on securing systems. These events can start with systems for a team to setup and secure. Alternately, organizers can provide already active systems that competitors must either protect, determine what is wrong with, or both. An example of a blue team event is the Collegiate Cyber Defense Competition [1], which is discussed below.

Red Team versus Blue Team Events – In this style of event, student teams with an offensive and defensive purpose are pitted against each other. Examples of red vs. blue style events include the Midwest Instruction and Computing Symposium's Red Team vs. Blue Team competition (in 2019 [47]) and DakotaCon's Cyber Conquest (planned for 2020 [48]).

Capture the Flag Events – Capture the flag style events are defined by the scoring approach: flag submittal. Individuals or teams solve puzzles, analyze logs, break into systems or take other actions. If they succeed, they are rewarded with a flag that they can submit to get points. Examples of capture the flag events include the National Cyber League [2] and MITRE CTF [4] competitions, which are discussed below.

Knowledge Competitions – Knowledge competitions test students on their retention or application of cybersecurity knowledge. An example of a knowledge competition is the US Cyber Challenge Cyber Quests [49], which is discussed below.

Tabletop Exercises – Tabletop exercises encourage students think or work through a problem with the use of role playing. Several currently available games would be appropriate for this including Control-Alt-Hack [50] and Backdoors & Breaches [51]. It is unclear if organized competitions for these or similar games have occurred.

4. Cybersecurity Competitions

This section provides several examples of regional and national cybersecurity competitions and briefly discusses their format. Table 1 provides website information for several of the competitions that are mentioned.

National Cyber League – The National Cyber League [2] is a capture-the-flag style competition for university and, more recently, high school teams. The competition has four parts. It starts with a 'gymnasium' where prospective players can learn and practice. Then, there is a qualifier round that places competitors into brackets. Next, there is an individual competition where students compete against both local and other students nationwide. Finally, a team competition allows students to group into teams (of changing sizes, from competition to competition) and compete against other teams. This competition is entirely online.

Collegiate Penetration Testing Competition – The Collegiate Penetration Testing Competition [46] is a U.S. nationwide competition with two rounds: regionals and nationals. In this competition, student teams take on the role of penetration testers and attempt to compromise and document the compromise of simulated client systems. This competition (both regionals and nationals) are in-person events.

Collegiate Cyber Defense Competition – The Collegiate Cyber Defense Competition [1] is a U.S. nationwide competition with three rounds: qualifiers, regionals and nationals. In this competition, student teams take the role of network administrators who must secure and maintain operations of computing resources. This competition has a hybrid location approach. At least some qualifiers and one regional are held online. Nationals is an in-person event.

Global Cyberlympics – The Global Cyberlympics is a category-spanning competition covering "digital forensics, web application exploitation, system exploitation, malware analysis, reverse engineering, cryptography and trivia" [52]. The competition is team-based and starts with an online qualifier round followed by an in-person final round.

Hivestorm Competition – Hivestorm [53] is an online competition, launched for the first time in 2019, that focused on blue team system security. The competition provided student participants with virtual machines that they downloaded. They then had to identify existing compromises of these systems and secure them.

Cyberforce Competition – Hosted by the U.S. Department of Energy, the CyberForce Competition [54] challenges student teams to secure energy-related computing systems. The competition is held onsite across multiple Department of Energy facilities, nationwide.

US Cyber Challenge Cyber Quests – The US Cyber Challenge Cyber Quests [49] is an online quiz-style competition. Student participants perform analysis of provided data and submit answers to a quiz based on what they've found.

Sponsored Competitions – A large number of cybersecurity competitions sponsored by corporations or other groups exist. Many of these are not targeted, specifically, at students. Students are welcome to participate; however, these may be appropriate only for advanced students. CTFTime.org lists numerous capture-the-flag style competitions [55]. The MITRE Corporation offers a STEM CTF [4] that is specifically targeted towards high school and college students (and has a separate students' bracket).

Table 1. Competition Details.

Competition Name	Details URL
National Cyber League	https://www.nationalcyberleague.org/
Collegiate Penetration Testing Competition	https://nationalcptc.org/
Collegiate Cyber Defense Competition	https://www.nationalccdc.org/
Global Cyberlympics	https://www.cyberlympics.org/
Hivestorm Competition	http://www.hivestorm.org/
Cyberforce Competition	https://cyberforcecompetition.com/
MITRE STEM CTF	https://mitrecyberacademy.org/competitions/
Cyber Quests	https://uscc.cyberquests.org/

Robotics Competitions Incorporating Cybersecurity Content – Having identified the critical nature of securing the command and control of robotics hardware, some robotics competitions are beginning to include security challenges. For example, the Intelligent Ground Vehicle

Competition has incorporated a challenge related to the NIST Risk Management Framework into its 2020 competition [56].

5. Student Outcomes

Anecdotally assessing student outcomes, it is clear that many of the benefits described in section 2 for problem-based learning do occur, to some extent, from competition participation. However, the competitions don't happen in a vacuum. Disambiguating the impact of competition participation from benefits provided by coursework and maturity gained due to aging and from other experiences in student participants is problematic.

Certainly, particularly with the National Cyber League – where explicit scorecards are provided, students advance notably from competition to competition, both in terms of their point score and by climbing up the ranks (even while the total number of competitors increases). In many cases, top student competitors also provide informal instruction to other students who are preparing for a competition for the first time or seeking to improve their performance. This peer-instruction likely is beneficial for both the student-instructor and student-learners.

Disambiguating the impact of competition familiarity, self-efficacy beliefs, gains made through other activities and gains made through competition preparation and participation is inherently problematic. Because the exact problems and materials covered change between competitions, even a knowledge / skill test might not fully quantify the change over time, much less the impact of the competitions themselves. Given this, student self-reported gain and gain-belief values become the only practical approach to assessing the efficacy of and benefits gained from these activities.

6. Assessing Student Outcomes

To assess the outcomes of student participants, a survey has been created. It is based on a survey that has been previously used to assess competition participation in other types of competitions (e.g., robotics [57]) as well as for peer-learning [58] and as a portion of assessing undergraduate research activities [59]. Before its initial use, in these other areas, it was validated with a relevant population of undergraduate and graduate students. This survey includes a number of key questions which include:

> *I am interested in seeking employment in the field that I participated in:*
>
> *I believe that participation will aid me in securing employment when graduating:*
>
> *On a scale of 1 to 9, please rate your technical skill in your area of focus before starting work on the project:*
>
> *On a scale of 1 to 9, please rate your level of comfort with the contest activities topic before starting work on the project:*

On a scale of 1 to 9, please rate your level of excitement with the contest activities topic before starting work on the project:

On a scale of 1 to 9, please rate your level of presentation skills before starting work on the project:

On a scale of 1 to 9, please rate your level of comfort with giving a presentation before starting work on the project:

On a scale of 1 to 9, please rate your level of leadership skills before starting work on the project:

On a scale of 1 to 9, please rate your level of leadership confidence before starting work on the project:

On a scale of 1 to 9, please rate your level of project management skills before starting work on the project:

On a scale of 1 to 9, please rate your level of time management skills before starting work on the project:

For the purposes of these questions, the term project is defined to include both the competition itself and the process of preparing for the competition. All of the above questions are assessed using a 9-point Likert-like scale. The questions with the word "before" in them also have a paired question that asks student respondents to indicate their status "at the present time" as well, which is used for comparison. Because student perceptions of their current state could change with their gain in knowledge from participation, students are asked to identify both their current and pre-participation levels at the same time (after participation). Because of this, the questionnaire quantifies how much students feel that they have gained in each area. The 9-point scales are captioned with relevant qualifying terms such as "very much", "a little" and so forth to ensure that the scale is perceived similarly by all respondents.

Respondents are also be asked about their participation time commitment, for basic demographic details, whether they had a leadership role (in team competitions) and their length of participation. They are also be asked about the benefits that they had hoped to achieve by participation and what benefits they actually received.

This survey will be used to assess cybersecurity competition activities during the coming year and beyond. An area of particular focus will be assessing National Cyber League participation, as this typically has the largest group size. Initially, this assessment will be deployed locally at North Dakota State University (NDSU). Secondarily, a wider-scale deployment is anticipated in conjunction with cybersecurity competition participation at other schools. It is planned that the survey will be administered to student participants in cybersecurity competitions electronically using Qualtrics within three days following the conclusion of the cybersecurity competition that they participated in.

The assessment of the survey will seek to identify what areas student competitors feel that they are obtaining benefit in and the comparative level of different types of benefits that they are attaining. It will also seek to identify what types of benefits competitors hope to attain when they are participating in cybersecurity competitions and how well these benefits are being delivered by competition participation. Finally, it will allow the comparative benefits of different types of competitions to be ascertained and it will facilitate comparisons of the time commitment and benefit levels produced by different competition formats. Appropriate statistical techniques, for the data being analyzed, will be used. In some cases, a basic t-test will be appropriate. In other cases, ANOVA and other more involved analysis will be required.

7. Conclusions and Future Work

This paper has reviewed the benefits from experiential education and problem-based learning, in general, from prior work. Technical, managerial and 'soft skill' benefits have been discussed. A number of different types of cybersecurity competitions have been presented and discussed. Multiple major student competition examples have been provided and described. A limited discussion of student outcomes from competition participation has been presented. Then, a quantitative study has been discussed and key questions from its instrument have been presented.

Future work includes the deployment of the quantitative survey instrument to competitors at NDSU and its prospective deployment, more widely, to competition teams at other schools. Longitudinal tracking of competition participants, both locally and at these other schools, is also planned. Assessment of this data will then be performed and reported on. The impact of cybersecurity competition participation will also be compared to participation in robotics competitions and other forms of experiential education.

Acknowledgements

Funding for student competition participation at NDSU has been provided by the NDSU Foundation as well as a variety of other sources. Thanks is given to all those who funded student competition participation and the participating students. Thanks is also given to several anonymous reviewers who enhanced this paper through their suggestions.

References

[1] "National Collegiate Cyber Defense Competition," *National Collegiate Cyber Defense Competition Website*, 2020. [Online]. Available: https://www.nationalccdc.org/. [Accessed: 20-Apr-2020].

[2] "NCL | National Cyber League | Ethical Hacking and Cyber Security," *National Cyber League Website*, 2020. [Online]. Available: https://www.nationalcyberleague.org/. [Accessed: 20-Apr-2020].

[3] "Cyber Cup Challenge | 2020 National Cyber Summit," *National Cyber Summit Website*, 2020. [Online]. Available: https://www.nationalcybersummit.com/Program/Cyber-Cup-Challenge. [Accessed: 20-Apr-2020].

[4] "MITRE Cyber Academy | Compete," *MITRE Cyber Academy Website*, 2020. [Online].

Available: https://mitrecyberacademy.org/competitions/. [Accessed: 20-Apr-2020].

[5] K. D. M. Snell, “The apprenticeship system in British history: the fragmentation of a cultural institution,” *Hist. Educ.*, vol. 25, no. 4, pp. 303–321, 1996.

[6] J. Straub, J. Berk, A. Nervold, and D. Whalen, “OpenOrbiter: An Interdisciplinary, Student Run Space Program,” *Adv. Educ.*, vol. 2, no. 1, pp. 4–10, 2013.

[7] G. Mountrakis and D. Triantakonstantis, “Inquiry-based learning in remote sensing: A space balloon educational experiment,” *J. Geogr. High. Educ.*, vol. 36, no. 3, pp. 385–401, 2012.

[8] N. Mathers, A. Goktogen, J. Rankin, and M. Anderson, “Robotic Mission to Mars: Hands-on, minds-on, web-based learning,” *Acta Astronaut.*, vol. 80, pp. 124–131, 2012.

[9] R. Fevig, J. Casler, and J. Straub, “Blending Research and Teaching Through Near-Earth Asteroid Resource Assessment,” in *Space Resources Roundtable and Planetary & Terrestrial Mining Sciences Symposium*, 2012.

[10] S. R. Hall, I. Waitz, D. R. Brodeur, D. H. Soderholm, and R. Nasr, “Adoption of active learning in a lecture-based engineering class,” in *Proceedings of the 32nd Annual Frontiers in Education Conference*, 2002, vol. 1, pp. T2A-9-T2A-15 vol. 1.

[11] D. R. Brodeur, P. W. Young, and K. B. Blair, “Problem-based learning in aerospace engineering education,” in *Proceedings of the 2002 American Society for Engineering Education Annual Conference and Exposition*, 2002, pp. 16–19.

[12] D. Broman, K. Sandahl, and M. Abu Baker, “The Company Approach to Software Engineering Project Courses,” *Educ. IEEE Trans.*, vol. 55, no. 4, pp. 445–452, 2012.

[13] S. Jayaram, L. Boyer, J. George, K. Ravindra, and K. Mitchell, “Project-based introduction to aerospace engineering course: A model rocket,” *Acta Astronaut.*, vol. 66, no. 9, pp. 1525–1533, 2010.

[14] N. Correll, R. Wing, and D. Coleman, “A One-Year Introductory Robotics Curriculum for Computer Science Upperclassmen,” *Educ. IEEE Trans.*, vol. 56, no. 1, pp. 54–60, 2013.

[15] M. Reynolds and R. Vince, “Critical management education and action-based learning: synergies and contradictions.,” *Acad. Manag. Learn. Educ.*, vol. 3, no. 4, pp. 442–456, 2004.

[16] C. F. Siegel, “Introducing marketing students to business intelligence using project-based learning on the world wide web,” *J. Mark. Educ.*, vol. 22, no. 2, pp. 90–98, 2000.

[17] R. C. Walters and T. Sirotiak, “Assessing the effect of project based learning on leadership abilities and communication skills,” in *47th ASC Annual International Conference Proceedings*, 2011.

[18] A. Ayob, R. A. Majid, A. Hussain, and M. M. Mustaffa, “Creativity enhancement through experiential learning,” *Adv. Nat. Appl. Sci.*, vol. 6, no. 2, pp. 94–99, 2012.

[19] Y. Doppelt, “Implementation and assessment of project-based learning in a flexible environment,” *Int. J. Technol. Des. Educ.*, vol. 13, no. 3, pp. 255–272, 2003.

[20] N. Hotaling, B. B. Fasse, L. F. Bost, C. D. Hermann, and C. R. Forest, “A Quantitative Analysis of the Effects of a Multidisciplinary Engineering Capstone Design Course,” *J. Eng. Educ.*, vol. 101, no. 4, pp. 630–656, 2012.

[21] F. Coffield, D. Moseley, E. Hall, and K. Ecclestone, *Learning styles and pedagogy in post-16 learning: a systematic and critical review*. London: Learning and Skills Research Centre, 2004.

[22] C. Manolis, D. J. Burns, R. Assudani, and R. Chinta, “Assessing experiential learning styles: A methodological reconstruction and validation of the Kolb Learning Style

Inventory," *Learn. Individ. Differ.*, vol. 23, no. 1, pp. 44–52, Feb. 2013.

[23] D. C. Kayes, "Internal Validity and Reliability of Kolb's Learning Style Inventory Version 3 (1999)," *J. Bus. Psychol.*, vol. 20, no. 2, pp. 249–257, 2005.

[24] M. Healey and A. Jenkins, "Kolb's Experiential Learning Theory and Its Application in Geography in Higher Education," *J. Geog.*, vol. 99, no. 5, pp. 185–195, 2000.

[25] D. T. Willingham, E. M. Hughes, and D. G. Dobolyi, "The Scientific Status of Learning Styles Theories."

[26] H. Pashler, M. Mcdaniel, D. Rohrer, and R. Bjork, "Learning Styles Concepts and Evidence," 2009.

[27] P. A. Kirschner and J. J. G. Van Merriënboer, "Do Learners Really Know Best? Urban Legends in Education," *Educ. Psychol.*, vol. 48, no. 3, pp. 169–183, 2013.

[28] M. Barclay, "Learning Styles: The Ugly Christmas Sweaters of Education | Franklin University," *I4 Blog*, 14-Feb-2017. [Online]. Available: https://www.franklin.edu/i4/blog/learning-styles-ugly-christmas-sweaters-education. [Accessed: 20-Apr-2020].

[29] C. Wee, M. Bashir, and N. Memon, "The Cybersecurity Competition Experience: Perceptions from Cybersecurity Workers," in *Proceedings of the Twelfth Symposium on Usable Privacy and Security*, 2016.

[30] M. H. Dunn and L. D. Merkle, "Assessing the impact of a national cybersecurity competition on students' career interests," in *SIGCSE 2018 - Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 2018, vol. 2018-January, pp. 62–67.

[31] J. Y. Oliver, J. Oliver, C. Elwell, C. Poly, and S. L. Obispo, "Effective Competitions for Broadening Participation in Cybersecurity," in *Proceedings of the 2018 ASEE Zone IV Conference*, 2018.

[32] P. Pusey, M. Gondree, and Z. Peterson, "The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations," *IEEE Secur. Priv.*, vol. 14, no. 6, pp. 90–95, Nov. 2016.

[33] J. M. Pittman, "Does competitor grade level influence perception of cybersecurity competition design gender inclusiveness?," in *SIGMIS-CPR 2015 - Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, 2015, pp. 49–54.

[34] D. Manson *et al.*, "The Cybersecurity Competition Federation: Promoting and connecting competitions into a developmental learning and enrichment experience," in *SIGMIS-CPR 2015 - Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, 2015, pp. 109–112.

[35] A. Mansurov, "A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching," *Mod. Appl. Sci.*, vol. 10, no. 11, 2016.

[36] M. Bashir, A. Lambert, J. M. C. Wee, B. Guo, and N. Memon, "Exploring the Vocational Interests of Cybersecurity Competition Participants | Journal of The Colloquium for Information System Security Education," in *Proceedings of the Colloquium for Information System Security Education*, 2015.

[37] J. Ming, C. Wee, M. Bashir, and N. Memon, "Self-efficacy in Cybersecurity Tasks and its Relationship with Cybersecurity Competition and Work-related Outcomes," in *Proceedings of the 2016 USENIX Workshop on Advances in Security Education*, 2016.

[38] M. Bashir, C. Wee, N. Memon, and B. Guo, "Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of

competitions as a recruitment tool," *Comput. Secur.*, vol. 65, pp. 153–165, Mar. 2017.

[39] K. Leune and S. J. Petrilli, "Using capture-the-flag to enhance the effectiveness of cybersecurity education," in *SIGITE 2017 - Proceedings of the 18th Annual Conference on Information Technology Education*, 2017, pp. 47–52.

[40] A. B. Woszczynski and A. Green, "Learning Outcomes for Cyber Defense Competitions," *J. Inf. Syst. Educ.*, vol. 28, no. 1, pp. 21–42, Nov. 2017.

[41] C. Eagle, "Computer security competitions: Expanding educational outcomes," *IEEE Secur. Priv.*, vol. 11, no. 4, pp. 69–71, 2013.

[42] R. S. Cheung, J. P. Cohen, H. Z. Lo, F. Elia, and V. Carrillo-Marquez, "Effectiveness of Cybersecurity Competitions," in *Proceedings of the International Conference on Security and Management*, 2012.

[43] M. Bashir, A. Lambert, J. M. C. Wee, and B. Guo, "An Examination of the Vocational and Psychological Characteristics of Cybersecurity Competition Participants," in *Proceedings of the 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education*, 2015.

[44] J. Hoag, "An Analysis of Academic Background Factors and Performance in Cyber Defense Competitions," *Inf. Secur. Educ. J.*, vol. 2, no. 1, 2015.

[45] R. Agada, J. Yan, and W. Xu, "A Virtual Animated Commentator Architecture for Cybersecurity Competitions," in *Advances in Intelligent Systems and Computing*, 2018, vol. 738, pp. 43–50.

[46] "Collegiate Penetration Testing Competition," *Collegiate Penetration Testing Competition Website*, 2020. [Online]. Available: https://nationalcptc.org/. [Accessed: 20-Apr-2020].

[47] "Cybersecurity Competition Rules – MICS 2019," *Midwest Instruction and Computing Symposium Website*, 2019. [Online]. Available: http://www.micsymposium.org/mics2019/cybersecurity-competition-rules/. [Accessed: 20-Apr-2020].

[48] "DakotaCon," *DakotaCon Website*, 2020. [Online]. Available: https://dakotacon.org/. [Accessed: 20-Apr-2020].

[49] "US Cyber Challenge: Cyber Quests Spring 2020," *US Cyber Challenge Website*, 2020. [Online]. Available: https://uscc.cyberquests.org/. [Accessed: 20-Apr-2020].

[50] "Control-Alt-Hack," *Control-Alt-Hack Website*, 2020. [Online]. Available: http://www.controlalthack.com/. [Accessed: 20-Apr-2020].

[51] "Backdoors & Breaches," *Black Hills Information Security Website*, 2020. [Online]. Available: https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/. [Accessed: 20-Apr-2020].

[52] "About the Games | Global Cyberlympics." [Online]. Available: https://www.cyberlympics.org/about-the-games/. [Accessed: 10-Feb-2020].

[53] "Welcome to Hivestorm," *Hivestorm Website*, 2019. [Online]. Available: http://www.hivestorm.org/. [Accessed: 20-Apr-2020].

[54] "CyberForce Competition^{TM} – A DOE Cyber Workforce Development Competition," *CyberForce Competition Website*, 2020. [Online]. Available: https://cyberforcecompetition.com/. [Accessed: 20-Apr-2020].

[55] "CTFtime.org / All about CTF (Capture The Flag)," *CTFTime Website*, 2020. [Online]. Available: https://ctftime.org/. [Accessed: 20-Apr-2020].

[56] "Official Competition Rules." [Online]. Available: http://www.igvc.org/rules.htm. [Accessed: 10-Feb-2020].

[57] M. A. Jones and J. Straub, “Robotic Competition Teams: Assessing the Experiential Education Value of Participation,” in *Proceedings of the 2019 ASEE Annual Conference & Exposition*, 2019.

[58] J. Straub, “Assessment of the Educational Benefits Produced by Peer Learning Activities in Cybersecurity,” in *Proceedings of the 2019 ASEE Annual Conference & Exposition*, 2019.

[59] J. Straub, “Experiential Research Education: A Report on the First Year of an NSF-sponsored Cyber-physical System Cybersecurity Research Experience for Undergraduates Program Experiential Research Education: A Report on the First Year of a NSF-sponsored Cyber-physical System Cybersecurity Research Experience for Undergraduates Program,” in *Proceedings of the 2019 ASEE Annual Conference & Exposition*, 2019.