Enhancing Computing Curricular Outcomes and Student Accomplishments Through Collegiate Competitions

Vijay Anand
University of Missouri-St. Louis
Saint Louis, Missouri, USA
vijay.anand@umsl.edu

Natalie A. Bolton
University of Missouri-St. Louis
Saint Louis, Missouri, USA
boltonn@umsl.edu

Prasad Calyam
University of Missouri-Columbia
Columbia, Missouri, USA
calyamp@missouri.edu

Rohit Chadha
University of Missouri-Columbia
Columbia, Missouri, USA
chadhar@missouri.edu

Rajendra K. Raj
Rochester Institute of Technology
Rochester, New York, USA
rkr@cs.rit.edu

Sumita Mishra
Rochester Institute of Technology
Rochester, New York, USA
sumita.mishra@rit.edu

ABSTRACT

Games and competitions enhance student engagement and help improve hands-on learning of computing concepts. Focusing on targeted goals, competitions provide a sense of community and accomplishment among students, fostering peer-learning opportunities. Despite these benefits of motivating and enhancing student learning, the impact of competitions on curricular learning outcomes has not been sufficiently studied. For institutional or program accreditation, understanding the extent to which students achieve course or program learning outcomes is essential, and helps in establishing continuous improvement processes for the program curriculum.

Utilizing the Collegiate Cyber Defense Competition (CCDC), a curricular assessment was conducted for an undergraduate cybersecurity program at a US institution. This archetypal competition was selected as it provides an effective platform for broader program learning outcomes, as students need to: (1) function in a team and communicate effectively (teamwork and communication skills); (2) articulate technical information to non-technical audiences (communication skills); (3) apply excellent technical and non-technical knowledge (design and analysis skills applied to problems-solving); and (4) function well under adversity (real-world problem-solving skills). Using data for both students who competed and who did not, student progress was tracked over five years. Preliminary analysis showed that these competitions made marginally-interested students become deeply engaged with the curriculum; broadened participation among women who became vital to team success by showcasing their technical and management skills; and pushed students to become self-driven, improving their academic performance and career placements. This experience report also reflects on what was learned and outlines the next steps for this work.

CompEd 2023, December 5–9, 2023, Hyderabad, India

ACM ISBN 979-8-4007-0048-4/23/12…$15.00
https://doi.org/10.1145/3576882.3617924

CCS CONCEPTS

• **Social and professional topics** → **Computing education programs**; **Student assessment**.

KEYWORDS

Experience report; college competitions; learning outcomes; assessment; student learning; problem solving; adversarial thinking; broadening participation.

ACM Reference Format:
Vijay Anand, Natalie A. Bolton, Prasad Calyam, Rohit Chadha, Rajendra K. Raj, and Sumita Mishra. 2023. Enhancing Computing Curricular Outcomes and Student Accomplishments Through Collegiate Competitions. In *Proceedings of the ACM Conference on Global Computing Education Vol 1 (CompEd 2023), December 5–9, 2023, Hyderabad, India.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3576882.3617924

1 INTRODUCTION

The use of games and competitions in computing education has been explored since the 1970s when the International Collegiate Programming Contest (ICPC) was launched. It currently is a multi-tiered innovative competition involving universities worldwide [5]. Such contests help engage students by providing experiential learning while providing a sense of community and accomplishment among students, faculty, and others involved.

Two related concerns, however, have been expressed about such competitions:

(1) Although aimed at broadening student participation, these competitions are typically focused on the strongest computing students, helping them increase and showcase their problem-solving skills, aptitude, and ambition [5], which may have adverse impacts on other students.
(2) Competitions are not integrated as a curricular approach that can impact and help a large number of students with diverse backgrounds within a program.

These concerns are directly addressed by our study. This experience report describes how competitions can motivate and enhance student learning for *all* students, not just the ones with adequate background and preparation needed to compete. We also investigate how competitions can be used as a supplementary assessment approach to evaluate the extent to which students are achieving course and program learning outcomes.

The competition used in our investigation is the Collegiate Cyber Defense Competition (CCDC) for conducting assessment activities for cybersecurity programs; the competition is described in more detail in Section 3. CCDC was appropriate for our purposes as it embodies the features we desire for detailed study and outcome analysis. To perform well in CCDC, students have to:

(1) Function in a team and communicate effectively (*teamwork and communication skills*).
(2) Articulate technical information effectively to non-technical audiences (*communication skills*).
(3) Apply excellent technical and non-technical knowledge and skills (*problem-solving, design, and analysis skills*).
(4) Function under adversity (*real-world problem-solving skills*).
(5) Take initiative to prepare for this extracurricular activity (*initiative*).

The setting for this project is a medium-sized state university in the United States Midwest, with an enrollment of approximately 10,000 undergraduate students and 1,000 graduate students. The reported student breakdown is approximately 60% women and 40% men, with around 8% black and 6% other minority groups. The average age of undergraduate students is 22 years. The average SAT score for incoming first-year undergraduate students is also 22. The four-year graduation rate is around 35%, and the six-year rate is almost 50%. In short, the university caters to reasonably motivated students representative of the undergraduate population in Computer Science nationwide and does a great job educating these students. As detailed in Section 5, competition participation was found beneficial in many ways, helping the students improve academically during their years in college and achieve successful careers after graduation.

Using data for both students who competed and who did not, this study tracked student progress over five years. Our data shows: (a) marginally interested students became deeply engaged with the curriculum; (b) competitions broadened participation amongst women who became vital to team success by showcasing their technical and management skills; and (c) students became self-driven, improving academic performance and career placement rates.

The rest of the paper is organized as follows. Section 2 discusses several games and competitions that we investigated to build our study. Section 3 discusses the relevant features of CCDC that make it useful for our investigation and Section 4 discusses the academic preparation needed for CCDC participation. Section 5 presents the results from the data collected for this study and the benefits we observed for our students. Section 6 reflects on what we learned and what we plan to do next.

2 RELATED WORK

The International Collegiate Programming Contest [5] is arguably the most familiar to computing faculty, given its international breadth and involvement. The 2022 ICPC Fact Sheet [4] mentioned that over 400,000 computing students tried to qualify to represent their universities. This resulted in almost 75,000 team members, coaches, and volunteers from over 3,450 universities in 111 countries on six continents participating for a chance to compete at the World Finals. The contest prides itself on attracting the strongest "cream of the crop". Although this contest also focuses on "creativity, teamwork, and innovation in building new software programs" and student performance under pressure, it is probably not appropriate for our modest needs to attract *broad participation of* students at all levels of expertise to competition-based learning [4].

In the field of cybersecurity, professionals and educators have used competitions to help students learn cybersecurity concepts. An early effort facilitated student access to an adequate infrastructure for formal teaching of cybersecurity concepts and an information security teaching model for institutions to train students in managing security risks through customized sandboxes [10]. Another effort adopted a cloud-based learning environment for students, 'V-Lab,' a reconfigurable and collaborative environment that features contained hands-on laboratory exercises for network security education using virtualization technologies [19]. Custom GUI web interfaces for management and a social site for knowledge sharing and contribution were developed. DeterLab [7] is similar, but at a much larger scale; it is more widely used for both cybersecurity research and education projects.

Another similar real testbed environment [12] was developed for cybersecurity teaching to overcome the lack of realistic simulation software; here, students can configure and run their networks and explore vulnerabilities, exploits, and remediation using a "cybersecurity professional's tool kit." Syracuse University's SeedLabs [3] have gained wide adoption worldwide and offer several hands-on security labs in the classroom setting. Another example of a formal teaching approach in a cybersecurity course is a virtual class environment to teach cybersecurity skills and cloud computing concepts using resources offered by Amazon Web Services [13].

Other efforts have focused on teaching cybersecurity concepts using competition-based student learning. In one such effort [11], the authors developed a movable server rack with dedicated networking components, along with laboratory exercises that offered practical scenarios to practice attack and defense strategies for "Capture the Flag" (CTF), which is a special kind of information security competition. Another effort [14] developed exercises for teaching ethical hacking and addressed issues such as Distributed Denial of Service (DDoS). Cybersecurity scenarios in a non-virtualized environment for CTF [17] had two teams perform attacks and defense of a given network, along with a Treasure Hunt where "attacking" students tried to find hidden treasures, such as files and passwords, in the network. Teaching ethical hacking techniques to defend against Denial of Service attacks in a secure virtualized environment has also been used [2].

Kos [6] presents a study of women participating in cybersecurity competitions and recommends improving such participation. The Women in CyberSecurity (WiCyS) organization is "dedicated to bringing together women in cybersecurity from academia, research, and industry to share knowledge, experience, networking, and mentoring" [18].

3 THE COLLEGIATE CYBER DEFENSE COMPETITION (CCDC)

As stated earlier, the Collegiate Cyber Defense Competition (CCDC) was used as an archetypal competition for conducting assessment

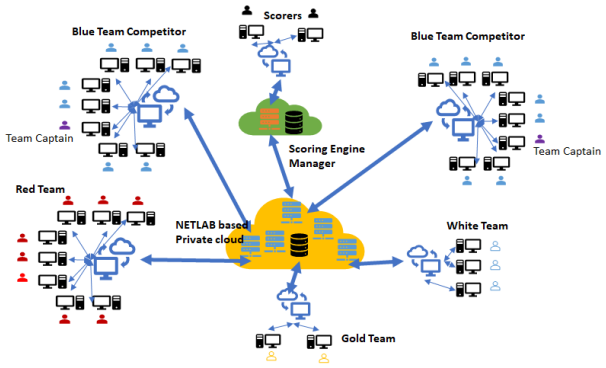

Figure 1: Overview of CCDC

activities for a cybersecurity program. CCDC is an annual competition first created and organized by the Center for Infrastructure Assurance and Security (CIAS) at the University of Texas, San Antonio 3. As the name suggests, CCDC is a cybersecurity defense competition. It was created to provide a platform (regardless of the institution's size) for cybersecurity students to have access to a uniform environment to practice their skills and compete against students at other institutions. The competition exercises are developed in collaboration with industry and government partners, enhancing the competition experience and ensuring the competition exercises' practical relevance. Salient features of the CCDC competition are described below while additional information can be found at the National CCDC website [16].

The competition measures the ability of a cyber defense team of students managing the security of a network and defending against active outsider threats, guaranteeing both availability and prevention of unauthorized access. The unique feature of CCDC, as opposed to other competitions, is that the exercises are held in a business environment and a team is scored both on its ability to defend as well as keep the business operational. A diverse range of skills is needed to succeed in such a competition. The operation of the competition is carried out using a NET- LAB [8] based private cloud. During the competition, each student team administers a virtual network that is supposed to mimic the operations of an IT company. For the smooth operation of the competition, the competition's management is organized into teams that have specific roles. An overview of the competition operation is shown in Figure 1. For the purposes of this paper, we highlight the relevant teams:

(1) *Blue Team.* Each competing team is called a blue team. A blue team consists of 12 students whom a faculty advisor mentors. Out of the 12 students, eight students participate actively in the competition and four students serve as alternates. At most two of the eight actively participating students can be graduate students and the rest are undergraduate students. During the competition, the blue team receives *inject requests* from the white team. These are requests for adding new network services, simulating the environment of a typical IT company. The team is led by a captain who is assisted by a co-captain. The captain is responsible for communication with the white team.
(2) *Red Team.* This team is drawn from industry professionals and plays the attackers' role. The team is responsible for targeting the defenses of the blue team, trying to either capture (virtually) resources protected by the blue team or place unauthorized files on devices protected by the blue team.
(3) *White Team.* The white team is also drawn from the industry and serves as competition judges. As part of the judging, they also provide the *inject tasks* for the blue team and evaluate the completion status of the tasks. Some white team members are responsible for ensuring the enforcement of the competition rules in each competition room (such as ensuring that the only hardware devices present are the ones provided by the competition) and do not serve as competition judges.
(4) *Gold Team.* The gold team is responsible for planning and administering the competition. It is composed of the Competition Manager, the host site Chief Administrator, and industrial and academic representatives.
(5) *Orange Team.* This team comprises student workers and professionals who assist in the evaluation of teams, by attempts to access internet-accessible services maintained by the blue teams as a regular user. The evaluation report is submitted to the white team which counts towards service scoring.
(6) *Green Team.* This team assists with any technical needs necessary to maintain the integrity of the competition.
(7) *Scorers.* A Scoring Engine Manager is responsible for keeping track of the scoring with the assistance of a scoring engine and scorers who take into account the completion of the inject tasks and the assessment of the blue team defenses by the red team.
(8) *Chief Judge.* A person who serves as the final authority on scoring decisions or issues related to equity or fairness of events or activities.

4 PREPARING STUDENTS FOR CCDC

To compete at CCDC, it is essential to understand the competition structure, as highlighted in Figure 2, which dictates how the team should be structured. It is also important to identify the necessary skills needed to be successful in the competition. The core courses provide content that helps students prepare for the competition, but it is inevitable that the students will have to gain skills beyond the classroom. As an example, the firewall component in Figure 2 can change over the years, and the firewall concepts taught in students' coursework might not be current, requiring extra preparation by the students in understanding the low-level details of the competition firewall administration. Thus, it is crucial to understand the nuances of team building and core coursework. The student performance data from the core coursework is then utilized for analysis. In the rest of this section, the students' academic preparation, including data collected for assessment, team structure, and other contributing factors for succeeding in the competition, are addressed.

4.1 Academic Preparation and Assessment Data

The program curriculum for the target group of students includes five core cybersecurity courses: one introductory level course, two

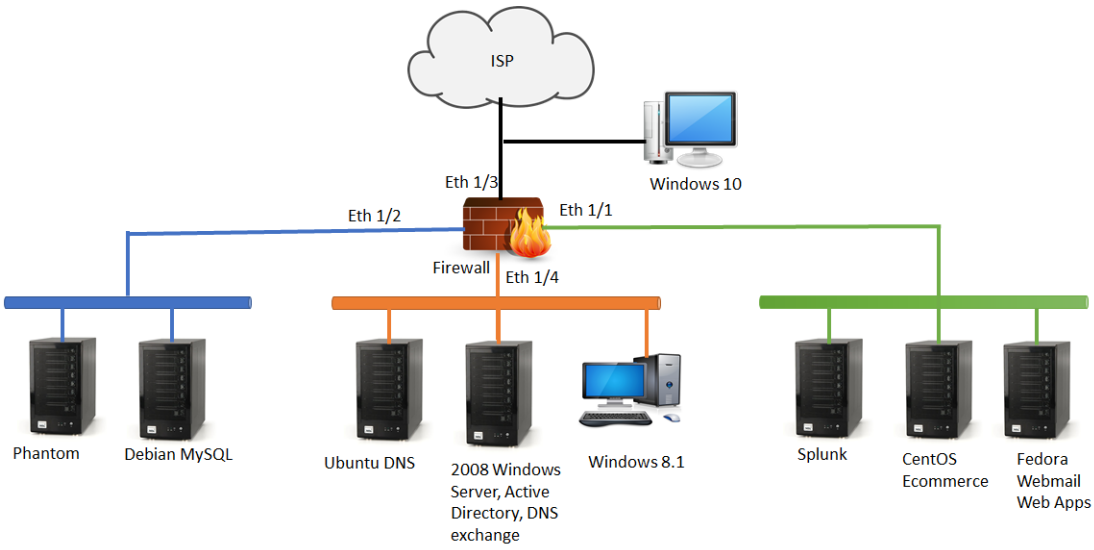

Figure 2: CCDC Competition Structure

intermediate level courses, and two advanced level courses. The introductory cybersecurity course introduces terminology, legal and ethical aspects, cryptography, malware, software security, policy definitions, network security, and forensic analysis. One of the intermediary courses focuses on a deep dive into secure programming, security compliance, threat modeling, risk analysis, applied cryptography, and security testing methods. The other intermediary course focuses on security principles, mathematical analysis of secure systems, security policies, and group management systems as applied to operating systems, networks, databases, and clouds.

One of the advanced courses focuses on computer forensics: media forensics, network forensics, malware analysis, and reverse engineering. The other advanced course focuses on web security, including cryptography, single sign-on, certificate authorities, secure web programming, deep dive into web vulnerabilities, secure eCommerce, and pen-testing web-based systems. Prerequisite knowledge required for these core classes includes requisite math that encompasses probability, statistics, and mathematical cryptography; programming, including application, web and assembly, operating systems, networking; and technical writing. The curriculum has been evaluated as a part of the US National Centers of Academic Excellence in Cybersecurity (NCAE-C) CAE-Cyber Defense (CAE-CD) designation requirements [15]. Beyond that, ABET also accredits the program using its criteria [1].

This study's data is from the grades given to students in different assessment types, e.g., exams, assignments, and projects. The grading distribution was as follows: Homework/Quiz 20%, Laboratory assignments/Presentations 20%, Midterm exam 25%, Final exam 30%, and class participation that accounted for attendance and other class interactions 5%. All laboratory assignments had to be submitted with documentation, and the documentation structure was provided. The data are, therefore, reflective of the students and program performance over the time period of this analysis.

4.2 Team Structure

The team structure is based on the technical challenges the students will face during the competition. As highlighted in Figure 2, the competition structure has a mix of services based on different flavors of Linux and Windows operating systems, a commercial firewall appliance, and a router. With such a diverse set of operating environments, the team needs to be divided into sub-teams addressing the broad areas of (1) experience and skills in the Linux operating environment and services associated with it, (2) experience and skills in Windows OS, and services, (3) networking skills and (4) communication skills to liaison with the white team in response to injects.

The team captain, typically belonging to one of these sub-teams, is also responsible for assessing the competition situation and directing mitigation resources as necessary. To support this dynamic structure of the sub-teams, each sub-team should be willing and competent to address challenges in other sub-team areas if the need arises. Proper coordination among the sub-teams is critical to completing tasks on time, and team dynamics become critical. To address this, students would typically practice cues of communication before the competition in simulated high-pressure competition situations.

With this framework in perspective, the implication for the competitors is: (1) All team members are competent to contribute to all sub-teams to mitigate various attacks they will encounter during the competition, (2) team members in their specific sub-team will have high skill levels in that tasks associated with the team, (3) all team members should communicate professionally with each other, and with the white team by gathering accurate technical facts and event details, (4) the liaison team that is typically entrusted with writing inject reports needs to have mature technical writing skills.

The students are divided into competitors and alternates: the former actively competes during the competition, while the latter fills in for competitors who fail to compete for any reason. As stated

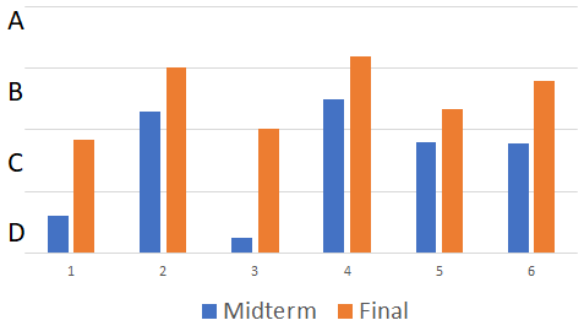

Figure 3: Performance of six marginal students before (midterm) and after (final) v participation.

earlier, the recommended number of competitors is eight, and the number of alternates typically is four. The competing team typically had second-year to fourth-year students and occasionally some exceptional first-year students while the alternates are primarily first-year students. We found this structure to provide continuity in team building as it formed a pathway of dissemination of lessons learned in the competition from experienced students to the first-year students, allowing for competing every year. To accommodate this student makeup, students would recruit teammates from their student club with some feedback from the faculty advisor.

4.3 Additional Team Performance Factors

Once teams are formed, the curriculum must provide computational support for practicing by experimenting with different competition constructs. When this data was collected, the students practiced within a private cloud infrastructure supported by the university.

To enhance the knowledge base, an effort was made to invite some industry experts to talk to the students or act as a red team for practice. Fortunately, many industry experts and program alumni made themselves available. This was a critical cross-cohort network-building exercise. Some of the program alumni subsequently hired students who participated in the CCDC.

5 EXPERIENCE REPORT

This experience report is based on the data collected over five years at the target higher education institution in the United States. The number of students in the program during this period of evaluation was approximately 150, of whom 35 students participated in the CCDC. This also accounts for the fact that a few students may join the CCDC group at a later stage, and some might drop off the team primarily due to the students' military deployments. Women constituted about 18% of the student base. International students consisted of approximately 8% of the student population. A few outcomes from the above data set related to the program are described in the following sub-sections.

Improvement in performance of marginally interested students. By marginally interested, we refer to students who enrolled in cybersecurity courses due to workplace demand. These marginally interested students became very involved in the program once they became a part of the competing team. This trend is highlighted in Figure 3, where we can see how the initial grade of the marginally

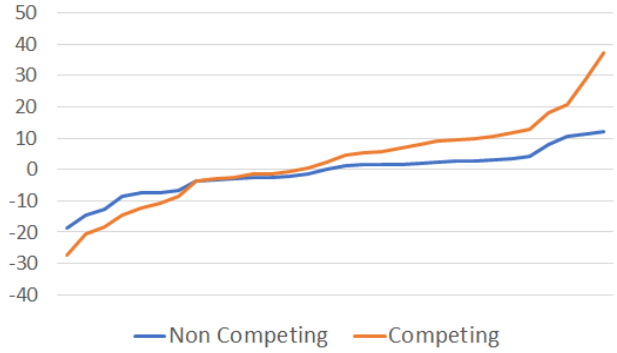

Figure 4: Comparison of randomly selected competitors (n=30, Avg Score 90.59) vs. randomly selected non competitors (n=30, Avg Score 83.87). The y-axis shows the score difference from midterm to final, and the x-axis shows students sorted in increasing order of score improvement.

interested at about the midterm improved over the semester. This shows significant effort from these students both in the classroom and beyond to enhance their skills. Among the 35 students who were a part of the competing team, five students fell into this marginal category.

Comparison of competitors with non-competing students. . The curricular performance of students who competed improved as the course progressed: it was significantly better than those of the non-competitors. The primary reason observed was peer learning, where competing students would cue non-competing students in labs and discussions, reflecting their improved understanding and skills gained via the extra-curricular learning in the competitions. This improvement can be seen in Figure 4, which shows how competitors improved their grades over a semester in an intermediate-level cybersecurity course. The t-test of the data of competitors (30 randomly selected students) to non-competitors (30 randomly selected students) yields a *p-value* of 1.34724E-10, showing statistically significant differences in their score improvement with competitors over-performing the non-competitors.

Program improvements. Student performance improved across the whole program. Competitors, when mixed with non-competitors in their respective courses, influenced those who did not compete positively. Figure 5 shows the average score of the non-competitors improved as they started taking the higher course levels. Many of the non-competitors would join the student club focused on the competition. This made the student club a powerful extracurricular platform for the program, where the faculty teaching core courses also participated as advisors. The graph also illustrates the beneficial effects of the presence of competitors on the non-competitors.

Women's participation. One of the notable observations was the impact the competition had on women's participation in the program. Women were an integral part of the competition team, and typically, the team overall had at least two women participants. Women were excellent competitors during the competition and demonstrated an excellent ability to manage team dynamics. This helped in team success. Among the five-year data that this study is

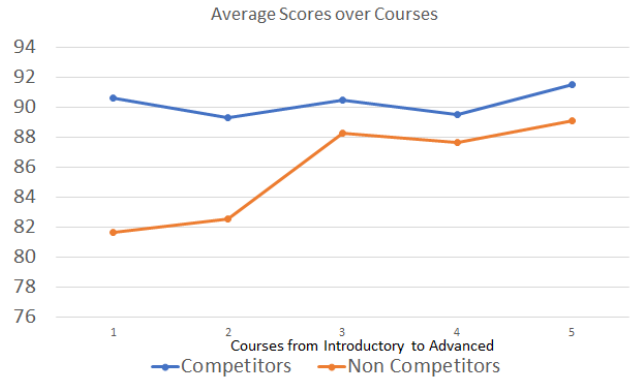

Figure 5: Progress of Competitors (n=35) and Non-Competitors (n=115) over five courses.

based on, women were team captains for two of those years. These women also held significant positions in the student cybersecurity club, including that of the club's president. Their representation in the competition team and their success brought other women into the program. The success stories of these women were highlighted in different university media channels. Consequently, the percentage of women in the program moved from 7% to 18% over five years, representing a significant improvement. Given the emphasis that CCDC places on collaboration, our experience confirms Kos's [6] findings that women can perform well when their collaboration styles can be brought out.

Improved career outcomes. Career success, including getting a job, is a primary student consideration, so competition substantially improves students' career prospects. Students who participated in competitions had at least one job by the time they graduated. Most competing students typically had two job offers. The students were placed in many premier private companies and niche private cybersecurity companies, along with several who chose to take up governmental positions. Some of the students continue to hold prestigious positions within the cybersecurity industry.

Lifelong learning influence. During their time as competitors, the students started to experiment with different operating environments, some of which were initially facilitated within the lab work. Subsequently, the competitors specifically, and other program students in general, started working on their own setup from reclaimed equipment. Although obtaining industry certifications was not the goal of the curriculum, many students got certified in different highly sought-after advanced cybersecurity certifications. Two students have published blogs on their exploits and have contributed their many exploits to `exploitdb` [9].

6 REFLECTIONS

Based on our five-year experience with preparing students for the CCDC described earlier, some preliminary observations can be made about the benefits of the use of competitions, not just for the best students in a program who participate in the ICPC [5], but *all* students in a program.

Students and Faculty. Moving out of campus to attend competitions brings new perspectives to students and faculty by exposing them to new and different ideas. Such networking and active exchange of ideas is a great learning experience for students and faculty. The positive impact on students has been discussed in the previous Section 5, but competitions also have a beneficial impact on faculty, who learn new things, get out of their comfort zone, and go on to make substantial program improvements.

Impact on Non-Cybersecurity Computing Programs. Although this study used CCDC and cybersecurity as the motivating competition, the world of competitions is broader than cybersecurity. Different kinds of hackathons focus on a variety of useful societal goals and could be useful for all computing programs to improve their curricular outcomes [6].

Meeting Program Requirements. As nearly all computing degree programs within the US are offered at regionally accredited institutions, program assessment is essential to establishing the continuous improvement processes required by the accreditor. Many programs are also accredited by ABET [1] whose criteria require a strong continuous improvement regime based on the assessment of student performance to see whether the program's student outcomes are being achieved by its graduates. If all students participate in appropriate competitions, the resulting data about student performance could be directly tied to ABET Student Outcomes relating to analysis, design, teamwork, communication, and professional conduct [1], thus providing a rich picture of the achievement of the student outcomes.

For cybersecurity programs offered at an institution designed as a US National Center for Academic Excellence in Cyber Defense (CAE-CD) [15], students are required to participate in cyber competitions and faculty participation to mentor them for such competitions on a regular basis.

7 CONCLUSION AND FUTURE DIRECTIONS

This experience report described a 5-year study conducted at a medium university that serves all kinds of students, not just the strongest. Given the number of universities that have participated in the CCDC over the years, future collaborations with other CCDC faculty advisors might provide the needed data for a more rigorous study. The results appear promising and warrant a more thorough investigation of whether the benefits of competitions, as described in this experience report, can be replicated at other institutions.

ACKNOWLEDGMENTS

Chadha acknowledges partial support from the National Science Foundation through Awards 1553548 and 1900924. Raj acknowledges partial support from the National Science Foundation through Awards 1922169 and 2110771.

REFERENCES

[1] ABET, Inc. 2023. 2023-2024 Criteria for Accrediting Computing Programs. https://www.abet.org/wp-content/uploads/2023/01/23-24-CAC-Criteria_FINAL.pdf.

[2] Shamma Al Kaabi, Nouf Al Kindi, Shaikha Al Fazari, and Zouheir Trabelsi. 2016. Virtualization based ethical educational platform for hands-on lab activities on DoS attacks. In *2016 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, New York, 273–280.

[3] Wenliang Du. 2011. SEED: Hands-On Lab Exercises for Computer Security Education. *IEEE Security Privacy* 9, 5 (2011), 70–73.

[4] ICPC. 2022. International Collegiate Programming Contest Fact Sheet. https://icpc.global/worldfinals/fact-sheet/ICPC-Fact-Sheet.pdf

[5] ICPC. 2023. International Collegiate Programming Contest. https://icpc.global/

[6] Brittany Ann Kos. 2019. Understanding Female-Focused Hackathon Participants' Collaboration Styles and Event Goals. In *Proceedings of the International Conference on Game Jams, Hackathons and Game Creation Events 2019* (San Francisco, CA, USA) *(ICGJ 2019)*. Association for Computing Machinery, New York, NY, USA, Article 5, 4 pages. https://doi.org/10.1145/3316287.3316292

[7] Jelena Mirkovic and Terry Benzel. 2012. Teaching Cybersecurity with DeterLab. *IEEE Security & Privacy* 10, 1 (2012), 73–76. https://doi.org/10.1109/MSP.2012.23

[8] Network Development Group, Inc. 2020. NETLAB+ VE Designated Operating Environment Guide. https://www.netdevgroup.com/support/documentation/netlabve/netlabve_designated_operating_environment_guide.pdf

[9] Offensive Security. 2023. Exploit Database. www.exploit-db.com

[10] Gordon W. Romney, Charles Higby, Brady R. Stevenson, and Nathan H. Blackham. 2004. A Teaching Prototype for Educating IT Security Engineers in Emerging Environments. In *Proc. of International Conference on Information Technology Based Higher Education and Training*. IEEE, New York, 662–667.

[11] Sebastian Roschke, Christian Willems, and Christoph Meinel. 2010. A security laboratory for CTF scenarios and teaching IDS. In *2010 2nd International Conference on Education Technology and Computer*, Vol. 1. IEEE, New York, V1–433–V1–437. https://doi.org/10.1109/ICETC.2010.5529213

[12] Julie A. Rursch and Doug Jacobson. 2013. When a testbed does more than testing: The Internet-Scale Event Attack and Generation Environment (ISEAGE) - providing learning and synthesizing experiences for cyber security students. In *2013 IEEE Frontiers in Education Conference (FIE)*. IEEE, New York, 1267–1272. https://doi.org/10.1109/FIE.2013.6685034

[13] Khaled Salah, Mohammad Hammoud, and Sherali Zeadally. 2015. Teaching Cybersecurity Using the Cloud. *IEEE Transactions on Learning Technologies* 8, 4 (2015), 383–392. https://doi.org/10.1109/TLT.2015.2424692

[14] Zouheir Trabelsi and Walid Ibrahim. 2013. Teaching ethical hacking in information security curriculum: A case study. In *2013 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, New York, 130–137. https://doi.org/10.1109/EduCon.2013.6530097

[15] US National Security Agenc. 2022. National Centers of Academic Excellence in Cybersecurity (NCAE-C). https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_designation_requirements.pdf

[16] UTSA Center for Infrastructure Assurance and Security (CIAS). 2020. National Collegiate Cyber Defense Competition (CCDC). https://www.nationalccdc.org/

[17] Giovanni Vigna. 2003. Teaching Hands-On Network Security: Testbeds and Live Exercises. *Journal of Information Warfare* 3, 2 (2003), 8–25.

[18] Women in CyberSecurity. 2023. Competition Opportunities. https://www.wicys.org/resources/competition-opportunities/

[19] Le Xu, Dijiang Huang, , and Wei-Tek Tsai. 2014. Cloud-Based Virtual Laboratory for Network Security Education. *IEEE Transactions on Education* 57, 3 (2014), 145–150.