NATIONAL CYBERWATCH CENTER

WHITE PAPERS

THE ROLE OF STUDENT COMPETITIONS IN CYBERSECURITY EDUCATION

AUTHOR: **JOHN SENER, SENER KNOWLEDGE LLC, APRIL 2016**

Contents

This paper describes the evolution of student competitions and their current role in cybersecurity education, articulates the potential of student competitions to support and improve cybersecurity education, describes issues regarding the expansion of student competitions and integration into cybersecurity education, and advocates for taking the role of student competitions to the "next level" in cybersecurity education.

I. Background

Cybersecurity Education

The rise of cybersecurity education has paralleled the increasingly critical importance of cybersecurity in society worldwide. In the US, there has been a dramatic increase in the attention paid to cybersecurity education, as illustrated by such initiatives as the White House Office of Cybersecurity, the National Initiative for Cybersecurity Education (NICE), and the Department of Homeland Security's development of new training standards [1]. This increased level of attention to the importance of cybersecurity education is in response to a general consensus that there is an acute shortage of qualified cybersecurity professionals. This has prompted calls for developing large-scale innovative cybersecurity education to develop an "agile, highly skilled workforce" capable of protecting and defending the nation's digital information and infrastructure from a "dynamic and rapidly developing array of threats" [2].

Among the goals of NICE are to accelerate learning and skills development that stimulate approaches and techniques to increase the supply of qualified cybersecurity workers more rapidly, "reduce the time and cost for obtaining knowledge, skills, and abilities for in-demand work roles," strengthen formal education programs, co-curricular experiences, and employer-based training, and explore tools and techniques that effectively measure and validate knowledge, skills, and abilities [3].

Student Competitions

Student competitions have a long, rich history at all levels of education. Some of them are relatively simple; for instance, numerous mathematics competitions are essentially multiple choice or problem-solving examinations [4, 5]. Other competitions, such as robotics competitions, can require extensive facilities and elaborate preparation. Many of them, from science fairs to MATHletes to Lego competitions, have gained both widespread participation, a degree of familiarity with their target constituents, and recognition by a wider community.

Student competitions provide participants a way to develop both technical or content-related skills and 'soft' skills, such as teamwork and time management. They are designed to be new, interesting, fun, and engaging; at the same time, many student competitions have a strong career-oriented focus, with the purpose of providing student participants with pathways, experiences, and connections for future career success. In the context of formal education,

student competitions are usually extracurricular activities, although they can often be integrated or even embedded into an educational curriculum.

Evolution of Cybersecurity Competitions

Cybersecurity competitions at the higher education level originated with the Cyber Defense Exercises (CDX), an inter-academy competition designed by the US military service in 2001. Student teams from the military service academies designed, implemented, managed, and defended a computer network against an attack team composed of security professionals from various government agencies [6]. This initiative prompted the National Science Foundation to sponsor a workshop with academia, government, and industry participants to discuss the possibility of developing a national cybersecurity competition based on the CDX and available to a broader audience of higher education students and participants. The result of this workshop was the development of the Collegiate Cyber Defense Competition (CCDC), which was first held in March 2005 at the University of Texas in San Antonio and included five Texas universities [7].

The success of the National CCDC resulted in its expansion through the creation of state and regional CCDC competitions, with the winners of the regional competitions qualifying to compete in the National CCDC competition. While the regional and National CCDCs have maintained their focus on "defense," more specifically the operational aspect of assuming administrative and protective duties for an existing network infrastructure [8], a host of other cyber competitions have arisen over the past ten years, including defense-oriented competitions, Capture the Flag (CTF), and forensics, among others [9]. Some examples:

DC3 Digital Forensics Challenge — Sponsored by the US Department of Defense's Cyber Crime Center, Air Force Office of Special Investigations, the DC3 Digital Forensics Challenge (most commonly known as DC3) started in 2006 as a global, online competition consisting of individual, progressive-level, digital forensic exercises. The DC3 challenge had several purposes, including promoting interest in digital forensics, establishing relationships within the digital forensics community, addressing major obstacles and dilemmas confronting digital forensics investigators and examiners, and developing new forensics tools, techniques, and methodologies. DC3 was a nearly year-long competition and accommodated teams from a wide variety of sectors: high schools, community colleges, undergraduate, post-graduate, civilian, commercial, US government, and US military [10]. The DC3 challenge ran through 2013, after which it was canceled because of the government shutdown and uncertainty about future funding sources [11].

CyberPatriot — At the high school level, the premier cybersecurity competition in the US is the National Youth Cyber Education Program, more commonly known as CyberPatriot. The first CyberPatriot competition was held in 2009 with seven Air Force Junior Reserve Officer Training Corps (JROTC) teams and one Civil Air Patrol team. Based on its initial success, CyberPatriot was expanded over the years to include teams from public and private high schools

in the US and abroad, and has grown tremendously in size and complexity to the point where over 3,300 teams registered to compete in the 2015-16 competition [12, 13].

National Cyber League — The National Cyber League (NCL) was founded in May 2011 with the goal of providing a training ground for collegiate students to develop and practice their cybersecurity skills though combined individual and team exercises. NCL's mission is to offer engaging, entertaining, measurable and scalable methods of learning to enlist a new generation of cybersecurity professionals. NCL seeks to differentiate itself from other cyber competitions by extending the timeframe for competitions through the use of environments that support yearround practice and competition for students at both the baccalaureate and community college levels. NCL is also different from other cybersecurity competitions in its intent to move beyond games and toward providing a "development league" that provides "resources for faculty and students to develop knowledge and validate skills" [14]. NCL has also grown to the point where over 2,150 students and over 300 faculty participated in the 2015 fall season [15].

II.Current Role of Student Cyber Competitions in Cybersecurity Education

Cyber competitions fulfill several important roles in cybersecurity education:

Learning experience — Cyber competitions help participating individuals develop cybersecurity skills [16]. As the National Initiative for Cybersecurity Careers and Studies (NICCS) notes, cyber competitions can include both technical skills and so-called 'soft' skills, and cyber competitions allow participants to practice, apply, and hone these skills in a "controlled, realworld environment" [16, 17]. There is some disagreement about whether cyber competition environments can in fact be accurately characterized as providing a "real-world" experience or whether these environments are actually highly artificial because they accelerate a contrived crisis. Nonetheless, student participants in cyber competitions such as the Mid-Atlantic CCDC (MACCDC) and the NCL have consistently reported learning on a wide variety of dimensions, including increased ability to apply technical skills and handle the pressure of real-world situations, improved individual 'soft' skills such as problem management and time management, improved interpersonal skills such as teamwork and communication, and greater insight into their personal strengths and weaknesses with regard to cybersecurity [18]. Collectively, and in some cases individually, cyber competitions can also accommodate various levels of ability from beginners to seasoned experts [19].

Motivating experience — Cyber competitions also help participating individuals increase interest in cybersecurity education and careers [16]. Survey, observational, and anecdotal data from numerous cyber competitions indicate that most participants consider their experience participating in cyber competitions to be highly motivating — extremely rewarding, fun, even a peak experience for some. Conversely, a cyber competition can be a way for students to learn

that a career in cybersecurity is not well-suited for them. For instance, a handful of students have reported such reactions in the annual MACCDC survey responses [18].

Integrating practical and theoretical experience — The fact that cyber competitions take place outside the traditional academic environment [19] is an important feature. For the most part, the traditional classroom environment remains an essentially content-driven, theory-based learning experience. Particularly in the field of cybersecurity, practical hands-on learning is an essential part of the educational experience and preparation for employment. Survey, observational, and anecdotal data from cyber competitions also indicate that participants greatly appreciate the practical, hands-on learning experience that cyber competitions provide. It is not uncommon for cyber competition participants to report that they learned more from participating in a single cyber competition than they learned from an entire semester or even year of coursework.

It is tempting to conclude from such reports that cyber competitions are an antidote or even a replacement for ineffective, out-of-date academic curriculum and teaching practices. However, this would be a misreading of the dynamic which cyber competitions are creating. In fact, **student competitions in cybersecurity education provide an excellent opportunity to integrate theory and practice by integrating extracurricular and curricular experiences.** Cyber competitions are an important complement to formal education because they require participants to use critical thinking and problem solving skills to complete tasks they have not seen in the classroom [20]. Cyber competitions also encourage "mentor-led atmospheres" [16] which enable faculty and students to work together in a specific context which is relatively rare in the traditional classroom experience. Student participants in the MACCDC and NCL competitions report that the events enable them to apply classroom learning to a real-world, hands-on experience. Faculty coaches and advisors also report that they have made changes to their classroom teaching practices based on their participation in these competitions, including adding more hands-on experiences to the classroom environment, integrating hands-on experiences and classroom learning effectively, and putting more emphasis on higher-order thinking skills such as analysis, synthesis, and critical thinking [18].

Cyber competitions can also serve as a way to introduce new content and skills to students, for instance by incorporating recent vulnerabilities and attack vectors which are too new to be addressed within a college curriculum [20].

Identifying and developing talent - Cyber competitions provide a new avenue for identifying and developing talent in potential cybersecurity professionals [16]. Student participants in the MACCDC and NCL competitions report that the experience enables them to be better prepared to work in the cybersecurity field. Many cyber competitions also provide additional venues for employers, students, and faculty to meet, such as job fairs, resume exchanges, and in some cases even direct recruiting for employment. More broadly, cyber competitions provide a venue for networking and information sharing, thus serving as an integral vehicle for entry into the cybersecurity professional workforce [17].

III. The Potential of Student Competitions to Support and Improve Cybersecurity Education

Cyber competitions have the potential to support and improve cybersecurity education in a variety of important ways.

Cyber competitions as "event-anchored learning" — Cyber competitions are a form of event-anchored learning: the use of an event or series of events to support, enable, or otherwise anchor a learning experience. Cyber competition events do this in several important ways: they engage participants, attract stakeholders, and add value to the entire process; they support the infusion of practical, hands-on learning activities and exercises into a curriculum; and they improve access and enable scale through virtualization [16]. In effect, cyber competition events function as nodes within a larger network of cybersecurity education-related activities; as events, they serve to attract a wide variety of activities which effectively support the network.

The MACCDC is an excellent case example. The MACCDC started in 2006 with five teams and 31 participants. In 2007, the MACCDC expanded from five to eight teams, then added a qualifying round and guest speakers in 2008. The following year, the qualifying round was virtualized, allowing the number of participating teams to increase from eight to 15; sponsor booths were also added to the in-person regional event. In 2010, a job fair was held during the in-person regional event, which resulted in much more contact with employers. These features enabled the addition of additional activities in ensuing years, including a High School Career Fair and Expo event, spectator component, and the use of the event as a source of research data (2011), as well as a live reporting component and coverage in a USA Today article (2012). These activities helped to grow the number of participants of all types, including student competitors, teams, faculty, potential employers, high school event participants, and sponsors [18].

As a result, the MACCDC started having an effect well beyond the event itself. Students began forming clubs to prepare for the MACCDC and other cyber competitions, and some of these clubs also started hosting other cybersecurity-related events as well. For instance, the University of Maryland cyber club reportedly had over 200 members, held a series of club events with featured guest speakers, and obtained corporate sponsorship for their participation in the 2010 MACCDC [21]. Perhaps even more importantly, faculty began to report that they were changing their classroom practices based on their participation in the MACCDC and other cyber competitions, for instance revising their courses and even creating new ones, in addition to the ways described above.

As a result of this dynamic, cyber competitions can positively impact cybersecurity education in a variety of areas:

Impact on Student and Program Development

Cal Poly Pomona professor Dan Manson expresses his vision of student and program development as a 50-50 rule. In Manson's experience, traditional classroom instruction comprises only about 50 percent of the value of an undergraduate education experience; the other 50 percent derives from extracurricular activities such as internships, participation in cyber competitions, and work experiences. Both are important, but the importance of extracurricular experiences is too often overlooked and underappreciated. However, participating in cyber competitions can help redress that imbalance and provide students with important opportunities to connect with the cybersecurity workforce community [22]. As a result, outreach efforts to provide these extracurricular activities are an essential part of developing a strong cybersecurity education program with a substantial student development component.

For example, cyber competitions provide the opportunity for students to form cybersecurity clubs for the purpose of preparing for competitions. This can be done in conjunction with faculty coaches or advisors, which provides opportunities for students to interact with faculty in enhanced ways that deepen the learning experience or in relatively new ways, such as collaborative knowledge creation. In addition, many student cyber clubs are student-led and/or student-run; this gives students additional opportunities to develop leadership, teamwork, communication, and other essential skills during the process of preparing for competitions as well as during the competitions themselves.

Cyber competitions also create new opportunities for students to gain valuable experience in other ways. For instance, college students are mentoring high school students, and high school students are mentoring middle school students who are participating in CyberPatriot competitions. It is becoming more common for students to participate in a competition and then become a mentor for that competition after they advance in their educational career.

Impact on Curriculum Improvement

Cyber competition experiences not only complement classroom learning but lead to opportunities for improving the curriculum by supporting the infusion of practical, hands-on learning activities and exercises into a curriculum. For instance, the NCL uses lab exercises which map to CompTIA Security+™ and EC-Council Certified Ethical Hacker (CEH)™ certification exams, which encourages more faculty to adopt existing lab exercises into their curriculum. Cyber competitions can also encourage the creation of new curriculum materials as well as the mapping of additional lab exercises and other curricular materials to industry competencies. Cyber competitions can also support the alignment of curricular materials to recognized competency frameworks such as NICE, and they can also support badging or other ways of certifying competencies demonstrated during competition events.

Impact on Faculty Professional Development

Cyber competitions provide faculty with opportunities to take on roles such as team coaches or advisors to prepare students for competitions. Faculty who participate in this role have reported that this activity was a valuable professional development experience in terms of influencing their teaching practices. For instance, faculty participants express gaining satisfaction from watching students respond to the challenges they faced, observing how they learned to work together as a team, watching them put theory into practice, and seeing how engaged they were in the experience. Faculty participants also report that they were able to work more closely with students in a way that wouldn't have happened otherwise, and they also gained insight into how to change their teaching to create a more effective learning experience [18].

Cyber competitions also encourage faculty to master new content or improve their skills so that they can be more effective teachers, coaches, and advisors.

Impact on Career Development

Students who participate in cyber competitions have also reported that their experience has had a significant impact on their future education and career plans. More specifically, many students in the MACCDC reported that they plan to take more courses, pursue a degree, or pursue a career in the cybersecurity field based on their experience. Occasionally, participating in competitions also has the opposite effect of convincing student participants that the field is not for them; however, this can also be seen as a positive outcome in terms of helping participants clarify their career goals before trying to enter the field. Similarly, competitions such as the NCL provide students with a chance to gain and demonstrate real-world skills, while the rankings, Scouting Reports, and skill metrics provide employers an opportunity to validate those skills and to recruit talent based on these performance-based assessments.

IV. Issues Regarding Expansion and Integration of Student Competitions into Cybersecurity Education

Although there is substantial evidence (experiential, anecdotal, participant surveys) that cyber competitions are playing an increasingly important role in cybersecurity education, there is a relative lack of empirical and other more formal research studies on the effectiveness of cybersecurity competitions, in particular for increasing interest and engagement in cybersecurity careers [23]. One related issue pertains to defining the "effectiveness" of cyber competitions. Arguably, the main goal of cybersecurity competitions is to produce individuals who are well-prepared to work in the field.

However, a broader view of the role of student competitions is also needed — one which acknowledges cybersecurity education as an ecosystem. Thus, the role of student competitions in supporting, growing, and nurturing the cybersecurity education ecosystem, for instance by

improving curriculum, developing faculty, and strengthening programs, is as least as important as measuring the success of cyber competitions in producing workforce-ready employees. Nevertheless, integrating cyber competitions into the cybersecurity career pathway is an important issue.

Integrating Cyber Competitions into the Cybersecurity Career Pathway

One related issue is whether cyber competitions are effective in engaging various types of participants. One exploratory study which reported initial results of one cyber competition consisting of three competition events found that participation among novice participants dropped between the first and third event. Related findings suggested the possibility that cyber competitions are effective in engaging participants who have prior experience in cyber competitions but are less effective in engaging novice participants. The study authors speculated that participants' engagement in cyber competitions may decline if they do not meet their performance expectations, or if they perform poorly relative to other competitors; however, they also note that more research is needed to explore these hypotheses [23].

Expanding opportunities for many more, or for a select few? Aerospace company Boeing's hiring of the entire winning team at the 2009 Western Regional CCDC [24] illustrates another related issue: do cyber competitions merely provide a convenient vehicle for companies to 'cherry-pick' the best and brightest prospects for employment, or do they provide a pathway which appreciably expands participants' opportunities for career employment and advancement? This is another area for which information is lacking, and both formal and informal research is needed. Although there is substantial evidence of a shortage of cybersecurity professionals [25], it is far less clear how that need can be met and the degree to which cyber competitions can play an important role in meeting that need.

Filling gaps in the cybersecurity career pathway? There are numerous gaps and disconnects in the cybersecurity career pathway system which exacerbate this issue. For instance, the Burning Glass report [25] found that almost 85% of cybersecurity postings specify at least a bachelor's degree and require at least three years of experience, based on analysis of online job postings. At the same time, practitioners in the field routinely assert that a prospective employee's skills are far more important on the job, and often in the hiring decision process, than degree attainment and prior experience. This disparity points to a likely disconnect between requirements determined by human resource departments and ones determined by practitioners in the field.

There is evidence that cyber competitions can help address the need to demonstrate and verify participant competencies in ways that meet employers' needs (as the Boeing hiring example illustrates). However, cyber competitions cannot directly address the educational attainment issue. Some work is also being done to determine the extent to which participation and demonstrated performance in cyber competitions can substitute for work experience.

Sustainability

Another related issue pertains to the sustainability of cyber competitions, both individually and as an ecosystem. As the DC3 competition illustrates, cyber competitions are often dependent on unreliable funding sources which can disappear as priorities change or larger events intervene. As with other successful ventures, cyber competitions are sometimes 'punished by success'; they often struggle with issues such as scaling up to accommodate increased demand, building human resources capacity, and building infrastructure capacity.

V. Future Directions: Taking the Role of Student Competitions to the "Next Level" inCybersecurity Education

There is abundant evidence to indicate that cyber competitions can find an even more important role in cybersecurity education — a "next level" in terms of having a more lasting impact on improving cybersecurity education. What might that next level look like? What future directions need to be pursued to reach this next level?

One future direction is to continue building an infrastructure of cybersecurity competitions that support student and program development, faculty professional development, curriculum improvement, and career development more effectively. Specific activities could include:

- Strengthening the linkages between student performance in competitions and documenting demonstration of performance relative to relevant skills and competencies;
- Developing more fully student development opportunities by participating in competitions in multiple roles (for instance, mentoring, coaching, Red Team, research);
- Getting employers to specify and recognize equivalent work experience values for demonstrated performances by participants in cyber competitions;
- Expanding the variety of industry-recognized skills sets, competencies, and certifications which are mapped to competition performances;
- Documenting and articulating the various ways in which faculty use competition participation and preparation to improve their curriculum and teaching and learning practices;
- Finding more ways to improve the persistence of novice participants by enabling them to compete and improve their skills more readily;
- Developing complementary alternatives to competition venues which allow participants to take advantage of the resources provided by student competitions without having to take part in the competition itself; and
- Creating a portable personal portfolio system which would allow students to collect, document, and share their accomplishments in multiple competitions.

Another possible future direction is to try to use cyber competitions more explicitly as a vehicle to address some of the more serious gaps and disconnects in the cybersecurity career pathway.

Acknowledgements

Thanks to Anna Carlin (California Polytechnic Institute, Pomona), Dr. Dan Manson (California Polytechnic Institute, Pomona), and Casey O'Brien (Prince George's Community College; National CyberWatch Center), for their review and comments which contributed to this paper.

References

[1] Bailey, T. and Sener, J. (2012). Impact of the NSF/ATE Cybersecurity Centers on the U.S. Cybersecurity Workforce. Presented at CISSE conference, Mobile, AL, June 2013.

[2] Jackson, W. (2011). Can the nation get smart about cybersecurity? GCN, August 12, 2011. Retrieved from:
https://gcn.com/articles/2011/08/12/nice-plan-for-cybersecurityawarenesseducation.aspx

[3] Newhouse, B. (2015). National Initiative for Cybersecurity Education. Federal Facilities Council Workshop, The National Academies of Sciences, Engineering, and Medicine. Retrieved from:
http://sites.nationalacademies.org/cs/groups/depssite/documents/webpage/deps_169707.pdf

[4] Mathematical Association of America (2016). AMC Contests. Retrieved from:
http://www.maa.org/math-competitions/amc-contests

[5] Wikipedia (2016). List of mathematics competitions. Retrieved from:
https://en.wikipedia.org/wiki/List_of_mathematics_competitions

[6] Hoffman, L. and Ragsdale, D. (2004). Exploring a National Cyber Security Exercise for Colleges and Universities. Report No. CSPRI-2004-08, The George Washington University, Report no. ITOC-TR-04001, United States Military Academy.

[7] White, G.B., and Dodge, R. C. (2007). The National Collegiate Cyber Defense Competition: What are the next steps? Proceedings of the 11th Colloquium for Information Systems Security Education, Boston University, Boston, MA June 4-7, 2007.

[8] National Collegiate Cyber Defense Competition (2014). History of CCDC. Retrieved from:
http://nationalccdc.org/index.php/competition/about-ccdc/history

[9] Manson, D. and Carlin, A. (2011). "A League of Our Own: The Future of Cyber Defense Competitions," International Information Management Association Journal, v.11. Retrieved from:
http://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1159&context=ciima

[10] Forensicswiki (2012). DC3 Digital Forensics Challenge. Retrieved from: http://forensicswiki.org/wiki/DC3_Digital_Forensics_Challenge

[11] Verton, D. (2013). Defense Cyber Crime Center cancels annual digital forensics competition. Fedscoop, October 9, 2013. Retrieved from: http://fedscoop.com/defense-cybercrime-center-cancels-annual-digital-forensics-competition

[12] CyberPatriot (2015a). What Is CyberPatriot? Retrieved from: www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx

[13] CyberPatriot (2015b). CyberPatriot: History. Retrieved from: https://www.uscyberpatriot.org/about/history

[14] National Cyber League (2015). Retrieved from: http://www.nationalcyberleague.org/about.shtml

[15] O'Brien, C. (2015). Wrapping up the Fall Season." December 15, 2015. E-mail

[16] NICCS (2015a). Promoting Education web page. Retrieved from: https://niccs.us-cert.gov/education/promoting-education

[17] NICCS (2015b). Cyber Competitions web page. Retrieved from: https://niccs.us-cert.gov/education/cyber-competitions

[18] Sener, J. (2013). Event-Anchored Learning: Using Cybersecurity Competitions to Engage Students. Sloan-C 6th Annual International Symposium on Emerging Technologies for Online Learning, Las Vegas, NV, April 11, 2013.

[19] NICCS (2015c). Cyber Competitions: Learn. Experience. Explore. Retrieved from: https://niccs.us-cert.gov/training/tc/search/cmp/new

[20] Pusey, P., O'Brien, C., and Lightner, L. (2014) Preparing for the Collegiate Cyber Defense Competition (CCDC): A Guide for New Teams and Recommendations for Experienced Players. National CyberWatch Press: 2014. Retrieved from: http://www.nationalcyberwatch.org/programs-resources/digital-press/

[21] O'Brien, C. (2016). Personal communication, February 15, 2016.

[22]. Manson, D. (2015). Personal communication, January 4, 2015.

[23] Tobey, D., Pusey, P., and Burley, D. (2014) Engaging learners in cybersecurity careers: lessons from the launch of the national cyber league. ACM Inroads, 5(1), March 2014, pp.53-56.

[24] Polycentric (2009). Boeing Hires Six Graduating Members of Cyber Security Team. Polycentric, October 11, 2009. Retrieved from: http://polycentric.cpp.edu/2009/10/boeing_hires_six_graduating_members_of_cyber_security_team/#.VqZ_DvGINmA

[25] Burning Glass Technologies (2015). Job Market Intelligence: Cybersecurity Jobs, 2015. Retrieved from: http://burning-glass.com/wp-content/uploads/Cybersecurity_JobsReport_2015.pdf

CYBERSECURITY EDUCATION
SOLUTIONS FOR THE NATION

National CyberWatch Center
Prince George's Community College
Room 129B
301 Largo Road
Largo, MD 20774

www.nationalcyberwatch.org

www.nsf.gov