An Argument for Game Balance: Improving student engagement by matching difficulty level with learner readiness

Portia Pusey, *National CyberWatch Center* David Tobey, Sr., *Indiana University South Bend*
Ralph Soule, *Naval Sea Systems Command*

Abstract

The exponential growth of students participating in cybersecurity competition and challenge programs has been used as support for claims that the numbers of students interested in pursuing cybersecurity careers are also increasing. However, one recent study documented a decline in novice participants over the course of three cybersecurity competitions. This paper presents an argument for supporting learner engagement by balancing the difficulty level of the game's activities with the learner's abilities.

1. Introduction

The time has come to add gaming slang such as *OP*, *nerf*, *2EZ*, *2M2H*, and *pwned* to the pedagogical lexicon of gaming in education. Gee, a researcher with extensive experience in games and learning asserts that "good games" can be "good learning" (2003, 2005, 2007, & 2009). However, bad games can drive players away because easy games leave players bored, while games that are too hard are frustrating (Csikszemtmihali, 1990; Prensky, 2001). Fundamentally, games are "problem solving spaces that use continual learning and provide pathways to mastery though entertainment and pleasure" (Gee, 2009, p. 67).

The difficulty in game design, and we would argue in gaming in education, is to provide pathways to mastery where the challenges are just within reach of a learner's ability to solve them so that competition activities remains "pleasantly frustrating" for the learner (Gee, 2005). However, "pleasantly frustrating" is difficult to achieve when one considers the broad range of possible abilities of the players or learners. Matching the difficulty level of the competition activities with a learner's abilities is what we mean by *game balance* for gaming in education. This paper presents an argument for supporting learner engagement in cybersecurity competitions by balancing the difficulty level of the game's activities with the learner's abilities.

2. Cybersecurity Competitions

The US Cyber Challenge review of cybersecurity competitions notes that many of the competitions provide an environment that assesses a moderate to high number of unique, advanced skills and do a good job of providing networking and employment opportunities (The Center for Internet Security, 2011). Anecdotally, the body of literature reports that cybersecurity competitions provide students opportunities to practice their skills and participate as a member of a team (Conklin, 2005).

Learning theory suggests that cybersecurity competitions when used in education can be a scaffold where novice and non-dominant groups collaborate to learn and develop their professional identities. "Learning is recognized as a social phenomenon constituted in the experienced, lived-in world, through legitimate peripheral participation in ongoing social practice; the process of changing knowledgeable skill is subsumed in processes of changing identity in and through membership in a community of practitioners; and mastery is an organizational, relational characteristic of communities of practice" (Lave, 1991, p. 64).

Qualitative studies describe that competitions support problem-based learning with authentic situations and can be motivating and promote knowledge development (Rosembloom, 2009; Wirt, 2012). Other findings regarding STEM competitions suggest that they could develop greater interest and enthusiasm among participants in topics related to competition (Lawrence, 2004; Mansaur, 2000; Tenable Security, 2011); provide students with the opportunity to apply knowledge from curriculum to real-world problems (Carter et al., 2008; Carter et al., 2011; Kearse & Hardnet, 2008; Pastor et al, 2008; Schweitzer et al., 2009), promote differentiation and enrichment of curriculum (Schacter, 2011; Campell, 2002), and encourage the development of teamwork and communication skills (Bowring, 2011; Carter et al., 2008; Carter et al., 2011; Kearse & Hardnet, 2008). Furthermore, competitions provide promotional opportunities for the field, career and educational institutions (Carter et al., 2008; Carter et al., 2011; Campell, 2002).

However, there is an absence of empirical studies of the effectiveness of cybersecurity competitions, which are critically needed if competitions are to be used in educational settings. Support for claims that cybersecurity competitions address the career pipeline is also lacking;

and evidence of increased interest in STEM careers from other related fields such as computer science and mathematics competitions have been not been conclusive, or in in many cases contradictory (Dede, 2009; Dede & Barab, 2009; Dede et al., 2005; Prenzel, 1992).

Schepens et al. (2002) assert that hands-on activities in the form of immersive educational simulations engage the learner, facilitate situational learning, and support the transfer of skills to everyday applications. Important longitudinal research on Science Olympiad success significantly correlates stronger proficiencies with the number of previous Science Olympiads attended and the number of relevant courses completed (Baird, et al, 1989). This suggests that learner capability and experience may be a factor in the success of cybersecurity competitions to engage learners and support the career pipeline. Potential cognitive and motivational effects were studied in a meta-analysis of serious games (Wouters et al., 2013). This study reported that there were no benefits to learning from using a serious game among students who were still in the process of developing foundational knowledge using drill and practice methods.

Furthermore, Cooper (2009) also found that a participant's level of ability may be a factor in engagement. This study reported that when ability is already high, participation in an immersive education simulation tool may increase engagement. Yet, this may not be true of novice learners. A recent exploratory study of a cybersecurity tournament, which consisted of three competitions over several months, reported that there was a substantial drop-off in novice participants across the three events (Tobey, Pusey & Burley, 2014). This may suggest that engagement or career interest may decline when a competitor (learner) does not perform up to their expectations, or performs poorly relative to other competitors (learners).

The implications of these studies for cybersecurity competitions used in educational settings are manifest. If, as these studies suggest, competitions increase engagement and are effective for students with high ability, the consequence is a learning experience which will only enhance the interest of those without need (or minimal need) of an instructional intervention. Therefore, it is critical that educators consider student capabilities when planning for educational competitions. These studies suggest that matching the competition activities with the existing skill sets of the students will provide for greater engagement and perhaps learning. This game balance is essential if cybersecurity competitions are to contribute to growth in learner capabilities, engagement and increasing the pipeline to cybersecurity careers.

3. Competence Development

Cybersecurity competitions, and those involved in cybersecurity professions, measure success based on an individual's competence (Tobey et al., 2012). This is a challenge for educators because research shows that competence-based professions, including healthcare, accounting and aviation, struggle with identifying and defining key competencies and the competencies of experts (Tobey, et al., 2012, Smith, et al. 2014). The competencies of experts are vastly different between beginners and experts. Moreover, there is a continuum of competencies between the beginners and experts which requires that instructional strategies change as a learner's capability increases (Ericsson 2008 & 2009). Since learning curves are steep in competence-based professions, knowing a learner's current capabilities informs the unique instructional strategies which are appropriate for their place in the beginner-expert competency continuum.

A purpose of cybersecurity competitions in education is to develop competent practitioners. The educational use of cybersecurity competitions is supported by the work of Brown, Collins and Duguid (1989) who assert that situated expertise becomes embedded through the interaction of declarative and procedural knowledge during skilled application. The key to this skilled application is diverse opportunities for practice, collaboration, and reflection which support the conversion of declarative and procedural knowledge into generalized and adaptive abilities.

The systematic process of practice, collaboration and reflection differs along the continuum of novice to expert competency. Therefore the educational experiences provided to novices, beginners and the proficient must vary as well. Prior to becoming an expert the problems presented to these developing learners must be well-defined so that the solutions can be found among established procedures and rules. An expert has developed causal models and situational awareness which enables them to solve unknown (ill-defined) problems.

The implication of the competency research on cybersecurity competitions is that the challenges, tasks, and competition activities must consider the proficiency of the competitor. This is especially critical when competitions are used in educational environments. In order to support the progression from beginner to expert, competitions need to differentiate activities to align with the problem-solving ability of the competitor (learner).

4. Learner Readiness

As an individual learns, reasons, and solves problems mental models and schemata are formed (Ifenthaler, 2010). Mental models "provide subjective plausible explanations on the basis of restricted domain-specific information" (2010. p. 82); these change over time. The mental models form the framework for connecting pieces of information about a topic into a single conceptual unit (Ifenthaler, Masduki, & Seel, 2011). For a beginner the framework of connecting pieces of information, which forms the cognitive structure, is sparse and has few links to related concepts. However, with instruction and practice, the beginner's cognitive structure becomes more like an expert's with many links between associated concepts (Ifenthaler, Masduki, and Seel, 2011).

It has been suggested that it is the complex cognitive structure which enables an expert to remain focused on valuable clues to solutions in complex, chaotic situations (Fuchs, Carpenter, Carroll, & Hale, 2011). Without sufficiently complex mental models for an unfamiliar domain, beginners struggle to identify clues to potential actions to solve advanced problems (Klein and Baxter, 2009). This suggests there are developmental readiness characteristics that are necessary in order for beginners to benefit from the intensive cognitive challenges included in many cybersecurity competitions.

5. Game Balance

In order for competitions in education to develop competency, the competition tasks must be aligned with a learner's abilities and readiness to solve the challenges. Formative assessment is the key to providing challenges that facilitate learning, and a key differentiation between play and games for learning. Formative assessment is used to improve teaching and learning (Bloom, 1968). For competitions in education this means evaluating students prior to, and during, the competitions to assure that the tasks are in line with their abilities and readiness, thus providing game balance.

Readiness must be evaluated across the full continuum of competence (Tobey et al. 2012). An evaluation should include measures of depth of understanding and include domain knowledge, consistency of the application of skills as well as the adaption of knowledge and skills to solve ill-defined problems (Johnsen, 2007; O'Neil et al. 2012).

Performance in educational cybersecurity competitions must be defined and measured based on a player's (learner's) stage of expertise development (Tobey, 2011). A formative assessment which informs game balance should involve four dimensions: 1) volatility, 2) uncertainty, 3) complexity, and 4) ambiguity, or VUCA (Chatham, 2009, Kiili, 2005, Johnsen, 2007, Wooters et al., 2013). Formative assessments that measure VUCA will indicate a learner's position on the learning curve and will identify which the tasks, methods, and tools should be used in the competition which align with a learner's readiness.

5. Conclusions

Cybersecurity competitions are serious games; they are contests of competence that seek to teach as well as engage (Garis, et al., 2002; Vogel, et. al. 2006). But there is evidence that while cybersecurity competitions attract a highly engaged population, they may not support novice players. In the gaming vernacular competitions that are ***2M2H*** (too much to handle) might leave a learner feeling ***pwned*** (like a loser). However, cybersecurity completions which have been ***nerfed*** (made easier) might be ***2EZ*** (too easy) for players who are ***OP*** (over powered) or experienced for the competition tasks. Therefore, we advocate for a multidimensional assessment that supports a game balance for learners of all abilities based on the four dimensions of VUCA (Johansen, 2007).

Competitions need to prioritize game balance especially if they are to be used in educational environments. Recent studies suggest that game balance is a key factor in increase engagement and career readiness (Cooper, 2009; Tobey et al., 2012). "A good teacher challenges her students, understands their struggles, and provides needed encouragement. A [good] game provides the same level of interaction, but with the added benefit of embedded assessments a student's progress is continually tracked" (Phillips, 2013). Furthermore, the assessments should guide adaptations to the challenges based on the current competence level of the competitor (learner). Future research should be done to determine if game balance helps to develop critical thinkers that become motivated to learn and engaged in cybersecurity careers.

6. References

Baird, W. E., Perry, W. D., & Simon, M., (1989). *Correlates of Student Performance in the Science Olympiad: The Test of Integrated Process Skills and Other Variables*. ERIC Document No. ED 305 248.

Bowring, J. F. (2008). A new Paradigm for Programming Competitions, in proceedings of SIGCSE'08, 87-91.

Bloom, Benjamin S. (1968). *Learning for mastery*. Los Angeles, USA: University of California press.

Brown, Collins, & Duguid (1989). Situated cognition and the culture of learning, *Educational Researcher*, 18, 32–42.

Campbell, J. R. (2002). Gender inequity among academic Olympians across the globe. *Journal of Research in Education*, 12, 75-79.

Carter, J., Bouvier, D., Cardell-Oliver, R., Hamilton, M., Kurkovskysta, S., Markham, S., McC.ung, O.W., McDermott, R., Riesdesel, C., Shi, J., & White, S. (2011). ITiCSE 2011 working group report: Motivating all our students. ITiCSE-WGR'11, June 27–29, 2011, Darmstadt, Germany.

Carter, J., Efford, N., Jamieson, S., Jenkins, T., & White, S. (2008). Taxing our best students, *ITALICS journal*, 7 (1),120-127.

Chatham, R. E. (2009). The 20th-century revolution in military training, pp. 27–60, in *Development of professional expertise: Toward measurement of expert performance and design of optimal learning environments*, New York: Cambridge University Press.

Conklin, A. (2005). The Use of a Collegiate Cyber Defense Competition in Information Security Education Information Security Curriculum Development (InfoSecCD) Conference '05, September 23-24, 2005, Kennesaw, GA, USA. Copyright 2005 ACM 1-59593-261-5/05/0009

Cooper, K. (2009) "Go with the flow: Engagement and learning in Second Life," presented at The Interservice/Industry Training, Simulation & Education Conference (I/ITSEC), Orlando: Florida.

Csikszentmihalyi, M. (1990). *Flow: The Psychology of Optimal Experience.* New York: Harper and Row

Dede, C. (2009). Immersive interfaces for engagement and learning. *Science*, 323 (5910), 66–69.

Dede, C., & Barab, S. (2009). Emerging technologies for learning science: A time of rapid advances. Journal of Science Education and Technology, 18(4), 301–304.

Dede, Chris, Honan, James P. & Peters, Laurence, C. (Eds.) (2005). *Scaling Up Success: Lessons Learned from Technology-Based Educational Improvement*. Jossey-Bass: New York.

Ericsson, K. A (2008), Deliberate practice and acquisition of expert performance: a general overview, *Academic emergency medicine*, 15, 988–994.

Ericsson, K. A. (2009). *Development of professional expertise: Toward measurement of expert performance and design of optimal learning environments.* New York: Cambridge University Press.

Fuchs, S., Carpenter, A., Carroll, M. & Hale, K. (2011). A hierarchical adaptation framework for adaptive training systems. In D.D. Schmorrow & C.M. Fidopiastis (Eds). Foundations of Augmented Cognition: Directing the Future of Adaptive Systems, pp. 413-421. Springer: New York.

Gee, J. P. (2003). *What video games have to teach us about learning and literacy*. New York: Palgrave Macmillan.

Gee, J. P. (2005). *Why video games are good for your soul: Pleasures and learning.* Melbourne, Australia: Common Ground.

Gee, J. P. (2007). *Good video games and good learning: Collected essays on videogames, learning, and literacy*. New York: Peter Lang.

Gee, J. P. (2009). Deep learning properties of good digital games: How far can they go? In U. Ritterfeld, M. Cody, & P. Vorderer (Eds.), *Serious games: Mechanisms and effects* (pp. 65–80). New York: Routledge.

Ifenthaler , D. (2010). Relational, structural, and semantic analysis of graphical representations and concept maps. *Educational Technology Research and Development*, 59(6), 817-840

Ifenthaler, D. , Masduki, I., & Seel, N.M. (2011). The mystery of cognitive structure and how we can detect it: Tracking the development of cognitive structures over time. *Instructional Science*, 39 (1), 41-61.

Johansen, Bob (2007). *Get There Early: Sensing the Future to Compete in the Present*. San Francisco, CA: Berrett-Koehler Publishers, Inc. pp. 51–53.

Kearse I. B. & Hardnett C. R. (2008). Computer science olympiad: Exploring computer science through competition, proceedings of the 39th SIGCSE Technical Symposium on Computer Science Education, Portland.

Kiili, K. (2005). Digital game-based learning: Towards an experiential gaming model, *The Internet and Higher Education*, 8 (1), 13–24.

Klein, G., & Baxter, H.C. (2009). Cognitive transformation theory: Contrasting cognitive and behavioral learning. In D. Schmorrow, J. Cohn, & D. Nicholson (Eds.). The PSI handbook of virtual environments for training and education: Developments for the military and beyond. Volume I: Learning, requirements and metrics. (pp. 50-65) Westport, CT: Praeger Security International.

Lave, J., & Wenger, E. (1991). *Situated Learning. Legitimate peripheral participation*, Cambridge: University of Cambridge Press.

Lawrence, R. (2004). Teaching Data Structures Using Competitive Games, *IEEE Transactions on Education*, 47 (4).

Mansaur, R. (2000). Hardware Competition in Engineering Education, IEEE 30th ASEE/IEEE Frontiers in Education Conference.

O'Neil, L. R., Assante, M. J., & Tobey, D. H. (2012). *SmartGrid Cybersecurity: Job Performance Model Report.* National Technical Information Service, Alexandria,VA, Technical Report PNNL- 21639.

Pastor, J., Gonzalez, I., Rodrigues, F.J. (2008). Participating in an international robot contest as a way to develop professional skills in engineering students, proceedings of the 38th Annual Frontiers in Education Conference, New York.

Phillips, V. (2013, March 8) "Learning grammar with a joystick and math with a mouse," Huffington Post.

Garris, R., Ahlers, R., & Driskell, J. E. (2002). Games, motivation, and learning: A research and practice model, Simulation & Gaming, 33, (4), 441– 467.

Rosenbloom A. (2009). Running a Programming Contest in an Introductory Computer Science Course, proceedings of ITiCSE'09, Paris.

Schacter, R. (2011). How are science fairs fairing? *District Administration*, 7 (9), 62-63.

Schepens, W. J., Ragsdale, D. J., Surdu, J. R., & Schafer, J. (2002). The Cyber Defense Exercise: An evaluation of the effectiveness of information assurance education, *The Journal of Information Security*, 1 (2).

Tenable Security (2011). *Resources for Team Preparation*. http://blog.tenablesecurity.com/2011/03/mid-atlantic-ccdc-lessons-learned-in-co mmunication.htm

The Center for Internet Security (2011). *U.S. Cyber Challenge: Assessment framework methodology* [Unpublished Manuscript].

Tobey, D. H. (2011). *A competency model of advanced threat response.* ATR Working Group Report NBISE-ATR-11-02. Idaho Falls, ID: National Board of Information Security Examiners.

Tobey, D. H., Pusey, P., & and D. Burley (2014). Engaging learners in cybersecurity careers: Lessons from the launch of the National Cyber League. *ACM Inroads: Special Section on Cybersecurity Education*.

Tobey, D. H., Reiter-Palmon, R., & Callens, A. (2012). *Predictive Performance Modeling: An innovative approach to defining critical competencies that distinguish levels of performance. OST Working Group Report.* National Board of Information Security Examiners, Idaho Falls, ID.

Vogel, J. J., Vogel, D. S., Cannon-Bowers, J., Bowers, C.A., Muse, K., & Wright, M. (2006). Computer gaming and interactive simulations for learning: A meta-analysis. *Journal of Educational Computing Research*, 34(3), 229-243.

Wirt, J. L. (2012). An analysis of Science Olympiad participants' perceptions regarding their experience with the science and engineering academic competition. *Dissertation Abstracts International Section A: Humanities and Social Sciences*, 72 (11-A).

Wouters, P., van Nimwegen, C., van Oostendorp, H., & van der Spek, E. D. (2013, February 4). A Meta-Analysis of the Cognitive and Motivational Effects of Serious Games. Journal of Educational Psychology. Advance online publication. doi: 10.1037/a0031311