Capture-the-Flag: Paradigm Utility for Enhancing Red Team Readiness

Tashara T. Cooper, Johnathan T. Harris
Naval Air Warfare Center Training Systems Division
Orlando, Florida
tashara.cooper@navy.mil
johnathan.t.harris@navy.mil,

ABSTRACT

U.S. Department of Defense (DoD) cyber test and evaluation (T&E) Red Teams face a myriad of challenges to training and maintaining readiness, and persistence of these challenges can place DoD cybersecurity assurance strategic goals and objectives at risk. DoD senior leadership is dependent upon adversarial assessment (AA) as a critical phase in the cybersecurity T&E process in order to mitigate risk to defense weapons systems, operational networks, and crucial data infrastructures. AA assesses the ability of a unit equipped with a system to support its mission while withstanding cyber-attacks characteristic of an actual adversary. However, cyber T&E Red Teams train as individuals despite AA being a team function. Additionally, availability of people to train (personnel), scheduling time to train (on-the-job), and opportunities for time to practice (on one's own) are shortfalls and challenges that the current training model of didactic instruction and sterile laboratory environments do not adequately address.

Ideally, improvements to the current training model would afford cyber T&E Red Teams with the opportunity to engage in realistic training akin to operational test environments at the team-level. Proposed is a game-based, offensive focused Capture-the-Flag (CTF) training paradigm. Capture-the-Flag is a team-based cybersecurity competition requiring execution of computer security and attack skills to solve a set of security challenges. CTF attempts to replicate real world systems or subsystems to practice both offensive and defensive cyber missions. By emulating the current threat landscape through offensive and defensive cyber missions, CTF supports cyber T&E Red Teams in maintaining behavioral and cognitive attributes required to maintain resiliency amidst changing tactics, techniques, and procedures (TTPs) of cyber-based adversarial attacks. Although there is variation in CTF design and deployment, the by-design pedagogical affordances the method offers supports the usefulness of CTF as an effective training option for DoD cyber T&E Red Teams.

ABOUT THE AUTHORS

Ms. Tashara Cooper is a research psychologist for the Naval Air Warfare Center Training Systems Division (NAWCTSD). She earned a B.A. in Education from Florida Atlantic University (FAU) as well as a B.S. in Psychology and Graduate Certificate in the Cognitive Sciences from the University of Central Florida (UCF). Ms. Cooper is currently pursuing two graduate degrees to include Instructional Design and Technology (emphasis in Instructional Systems Design) and Modeling & Simulation (emphasis in Human Systems). Her areas of interest include training effectiveness evaluation, flexible course/instructional design, supportive human performance technologies, and human performance measurement and evaluation. She has supported basic and applied research in intelligent tutoring, adaptive training, culture and trust, and intuitive decision-making. Currently, she supports the Office of Naval Research (ONR) Human Performance Training and Evaluation initiatives, fiber optics training for P-8A platforms, application of augmented reality (AR) innovative training solutions for the Aircrew Survival Equipmentman, and cybersecurity Capture-the-Flag training paradigm.

Dr. Jonathan Harris is a software developer and cybersecurity researcher for the Naval Air Warfare Center Training Systems Division (NAWCTSD). He earned his Ph.D. in Industrial Engineering from the University of Central Florida (UCF), where his research focus was human assessment. His areas of interest include cybersecurity, training, and Live, Virtual, and Constructive (LVC) interoperability. Dr. Harris currently leads several projects in support of Department of the Navy (DoN) Modeling and Simulation (M&S), multiple Department of Defense (DoD) National Cyber Range (NCR) complex Capture-the-Flag exercises, and Navy Continuous Training Environment's Digital Radio Management System (DRMS).

Capture-the-Flag: Paradigm Utility for Enhancing Red Team Readiness

Tashara T. Cooper, Johnathan T. Harris
Naval Air Warfare Center Training Systems Division
Orlando, Florida
tashara.cooper@navy.mil,
johnathan.t.harris@navy.mil

INTRODUCTION

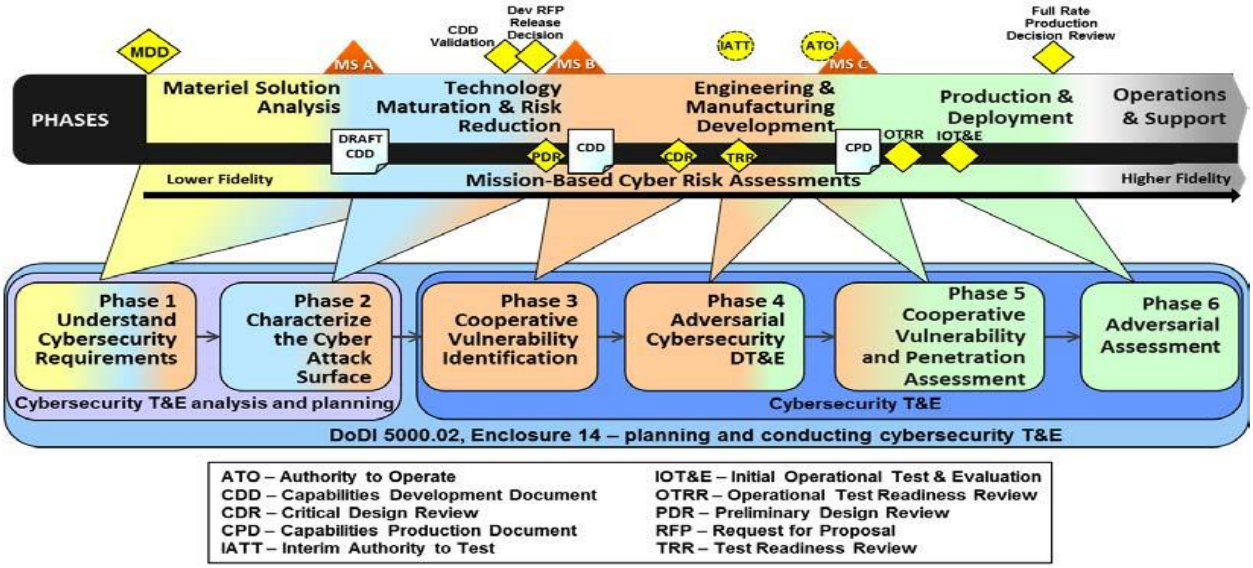
Growth in computerized interconnectivity, automation, and data collection capabilities is both a benefit and a challenge to government, industry, and academia. Each of these organizations can leverage such capabilities to increase administrative and operational efficiencies (Government Accountability Office [GAO], 2018). For example, automation of administrative tasks and operational controls can accelerate organizational processes and result in increased productivity. In addition, use of these capabilities can augment data collection and analysis functions to improve product development and delivery through removal of anomalies ((Ernst &Young, 2020; Pricewaterhouse Coopers, 2018). For the Department of Defense (DoD) specifically, extended system and network connectivity affords deeper integration and improved interoperability of live, virtual, and constructive (LVC) warfighting capabilities. However, the increase in more software dependent and network-connected weapons systems and subsystems introduces a new set of vulnerabilities. With the introduction of new vulnerabilities, new barriers and challenges to weapons systems cybersecurity are also introduced requiring DoD senior leaders to reassess its cybersecurity defense position (GAO, 2018).

Although modernized capabilities have become a vital component of the DoD present day military posture, greater automation and interconnectivity between and across systems changes the nature and type of cyber threats and attacks. Modernized technology enables adversaries the benefit of a greater attack surface, as well as, access to more advanced resources to deploy more creative, highly sophisticated tactics, techniques, and procedures (TTPs) on a weapons system (at an increased rate) making it difficult to detect, deter, prevent, or remove them (Ernst & Young, 2020; GAO, 2018). The DoD has employed weapons systems cybersecurity policy, guidance, and initiatives to improve its cyber hygiene; however, the effectiveness of these measures is impacted by limitations and challenges associated with personnel, information sharing, and systems (and sub systems) test and evaluation that represents the full range of vulnerabilities (GAO, 2018). In terms of testing, given there are known, as well as, unknown threats to a system; it is a major feat to test 100% of all threats. Therefore, DoD cybersecurity T&E professionals can only test 100% of the known and not the unknown threats. Thus, 'right size' testing that addresses the most critical known threats to a system is plausible. Leveraging the National Institute of Standards and Technology (NIST) Risk Assessment Guide to inform the DoD's Risk Management Framework (Figure 1) and its Cyber Test and Evaluation (T&E) activities is a step in the right direction toward conducting 'right size' testing (DoD 2020).

The DoD's Risk Management Framework (RMF) includes developmental test and evaluation (DT&E), as well as operational test and evaluation (OT&E) activates. As shown in Figure 1, cybersecurity T&E mapped to the DoD's Acquisition Process exists as part of all six phases. Phases 1-4 represents DT&E activities. During these phases, the goal is early discovery of system vulnerabilities. The early discovery of system vulnerabilities facilitates remediation of identified threats to system performance and reduces negative impacts to cost, schedule, and performance. On the other hand, Phases 5-6 represents OT&E activities. During these phases, the goal is supporting evaluation of system effectiveness, suitability, and survivability. Mission success is reliant on prevention of cyber threats, mitigation of cyber-attacks, and resilience recovery from a cyber-attack in preparation for the next fight (DoD, 2020). A team of testers performs DT&E and OT&E activities to include vulnerability assessments, security controls testing, penetration and adversarial testing. As a collaborative unit, Blue Team (DT&E) and Red Team (OT&E) testers engage in verification and validation of cybersecurity capabilities, assessments, and resiliency across the life cycle of a system (DoD, 2020).

Figure 1

Cybersecurity Test and Evaluation Mapped to the Acquisition Process



As seen in Table 1 below, Blue Teams are defensive focused. Their area of responsibility is maintaining a resilient security posture against a group of artificial attackers (i.e., the Red Team). Blue Team and its supporters must defend against real or simulated cyber-attacks in order to defend an enterprise's use of information systems. Blue Team defense activities (a) take place over a significant timeframe, (b) must occur in an environment representative of the operational context (e.g., operational exercise), and (c) must adhere to established and monitored rules of engagement by the neutral White Team (DoD, 2020, Defense Acquisition Guidebook [DAG], 2017).

Table 1

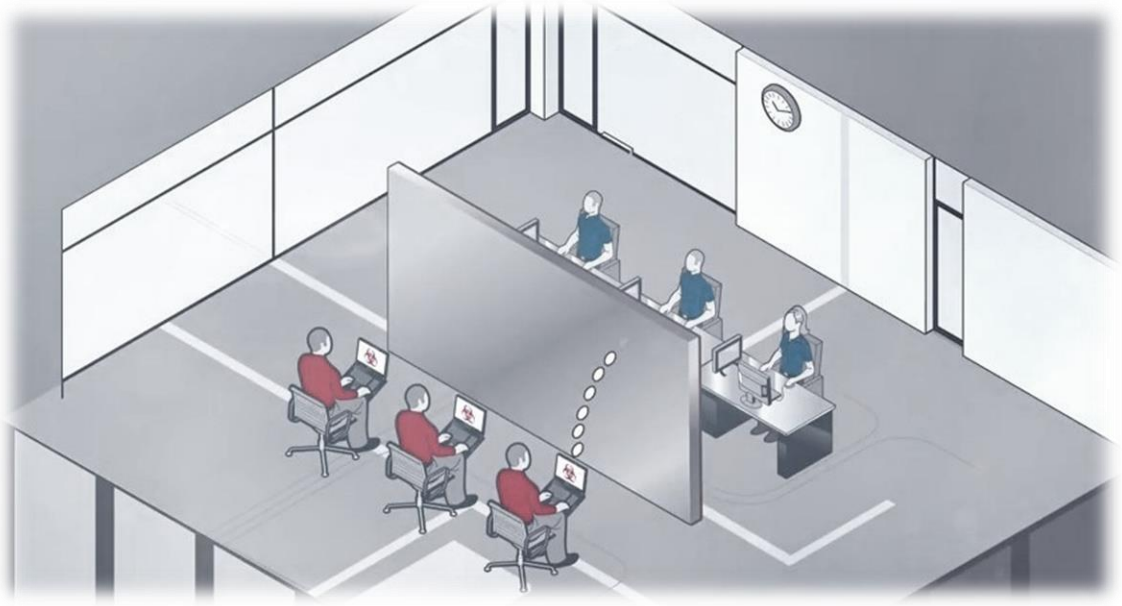
Cybersecurity and the Acquisition Life Cycle Integration Tool (CALLIT, DAU 2018)

Vulnerability Assessment (Blue Team)	Threat Representative Testing (Red Team)
Comprehensive	Exploit one or more known or suspected weaknesses
Identifies any/all known vulnerabilities present in systems	Attention on specific problem or attack vector
Reveals systemic weaknesses in security program	Develops an understanding of inherent weaknesses of system
Focused on adequacy & implementation of technical security controls and attributes	Both internal and external threats
Multiple methods: hands-on testing, interviewing personal, or examination of relevant artifacts	Model actions of a defined internal or external hostile entity
Feedback to developers and system administrators for system remediation and mitigation	Report at the end of the testing
Conducted with full knowledge and cooperation of systems administrators	Conducted covertly with minimal staff knowledge
No harm to systems	May harm systems and components & require clean up

On the other hand, Red Teams (Table 1) are adversarial actors. DoD Red Teams are independent, multi-disciplinary, certified and accredited personnel. They are authorized to employ adversarial TTPs on DoD networks and systems. They emulate potential adversary attack and exploitation methods against a system's current cybersecurity posture. These efforts help to improve an enterprise's Information Technology (IT) cybersecurity posture and Blue Team defense TTPs in an operational environment (DoD, 2020; DODIG, 2020). Despite criticality of activities performed, Red Teams face educational and training challenges. As a mission essential subset of the cybersecurity workforce, Red Teams have specific training requirements in offensive cyber operations not satisfied by classroom training or academic programs alone. Although an asset, university degrees and industry certifications are insufficient as end-points for determining Red Team proficiency or as a metric for translating quality of job performance (Schab, 2017). Personnel challenges such as attrition and turnover rates means not enough people to train and a degradation in useful knowledge management related behaviors like knowledge sharing and transfer. Figure 2 illustrates a notional test environment. Although the illustration is notional, it provides a graphical view into the team-based collaborative nature of T&E.

Figure 2

Notional Test Environment (Based on Panini, 2018)



Although the illustration is notional, it provides a graphical view into the team-based collaborative nature of T&E. Upsets to DoD cybersecurity T&E Blue and Red Team's ability to function as an effective unit, whether its personnel, education, or training related, represents a real training need. Red Team activities support not only a more resilient cybersecurity posture, but also augments Blue Team defense capabilities. Innovative training methodologies that are offensive-focused, train at the team level, encourage beneficial knowledge management elements, target relevant KSAs, require use of core cognitive capacities, employ variable instructional strategies, and include realistic characteristics of the actual operational environment have the greatest potential to support Red Team readiness. By design, Capture-the-Flag is a plausible approach to support factors that facilitate effective cybersecurity test and evaluation functions

CAPTURE-THE-FLAG: OVERVIEW, AFFORDANCES, AND ATTRIBUTES

Capture-the-Flag (CTF) is a team-oriented competitive game. Traditionally, these games occurred as an indoor or outdoor physical activity. Today, they have become a way to train cybersecurity concepts and skills. Government, industry, and academia have utilized some variation of a cybersecurity CTF as an education or training tool. These

organizations make use of a Jeopardy-style, attack-defend, or mixed mode defensive/offensive-focused cyber CTF (Davis, 2020; McDaniel, Talvi, & Hay, 2016; Namin, Aguirre-Muñoz, & Jones, 2016). In the CTF, current attacks can be simulated, enterprise IT systems (and sub-systems) can be modeled, and the attack sequence can be mapped to relevant cybersecurity T&E KSAs (at various skill levels).

Furthermore, designers can integrate a variety of pedagogical methods to encourage the application of higher order thinking skills. The cyber CTF offers a safe environment for Red Teams to validate, refine, and develop TTPs through hands-on experiences for carryover into the operating environment. Literature on CTF typically focuses on either how to organize and run a CTF or lessons learned. However, this paper focuses on the benefits of an offensive-focused Cybersecurity Capture-the-Flag (CTF). More specifically, how the by design affordances and attributes of CTF can address gaps in current training to augment Red Team readiness.

Traditional formats of CTF require the use of skills such as physical speed, stealth, endurance, strategy, and observation (Ford, Sirai, Haynes, & Brown, 2017). In such a format, players attempt to capture the opposing team's flag/s and transport it/them safely back to their respective territory. Traditional CTFs have taken place globally, as well as, in space (Strickland, 2020; Chain, Kuo, Liu, Li, & Yang, 2018; Huang, Ding, Zhang, & Tomilin, 2011). Currently, three styles (Jeopardy, attack-defend, and mixed mode) of CTF have risen as a popular way to train cyber security skills via computer-based means in a variety of settings around the world. Mental speed, stealth (flexibility), control, and endurance are the skills required during computerized versions of CTF.

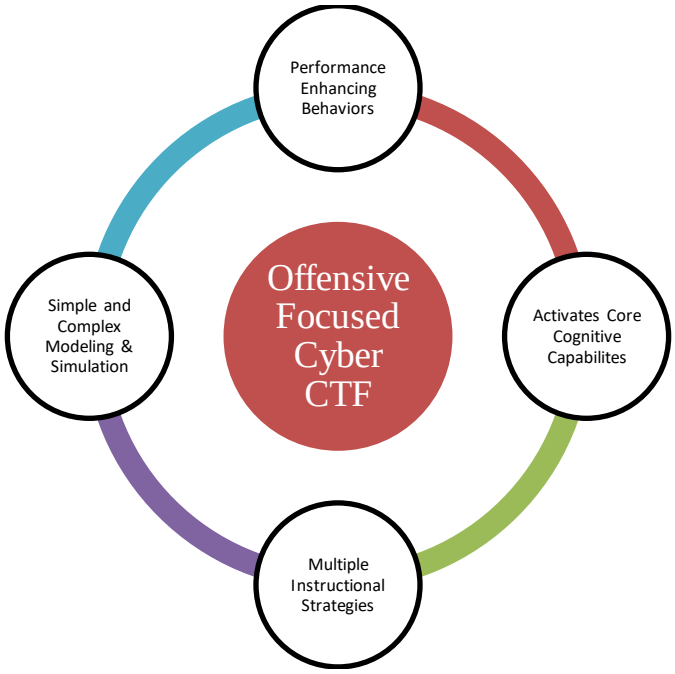
In Jeopardy-style CTFs there can be more than two teams because there is no attack-defend aspect to the game. However, in attack-defend or mixed mode (the attack-defend portion), each team attacks the opposing team's system while simultaneously defending their own system (Radcliffe, 2007). In these environments, flags are data files and teams utilize hacking tools (provided and/or homemade) in adherence with established rules of engagement within a pre-determined duration of time. Cyber security CTFs are flexible in design, in fidelity, goals and objectives, and in the KSAs targeted.

In the realm of DoD cyber T&E, Red Team rotational assignments, personnel turnover, and attrition rates affect availability of people to train (Schab, 2017). Resulting personnel deficits due to such factors reduce on-the-job training and time for practicing needed skills. These deficits lead to a degradation in Red Team knowledge management – that is it impairs the sharing and transfer of knowledge among team members. Additionally, under the traditional model, teams often train as individuals despite the fact that cyber security assessment and evaluation activities are a collective team function. Therefore, training that builds on teamwork is a way to promote the sharing and transfer of knowledge within the team. A cyber security CTF is an ideal platform for a team to work on functioning more cohesively as a unit through the sharing and transfer of knowledge occurring during completion of challenges. Cyber T&E is a high criticality function, so practice in a safe and low-risk training environment as a unit is critical to information and operational security.

Cyber security CTFs offer teams the opportunity to test and vet commercial or homemade developed hacking tools. The test and vetting of hacking tools can either take place in a low or in a high fidelity training environment. Low fidelity CTFs can use virtualized hardware in the cloud, whereas high fidelity CTFs can utilize the power of a cyber-range. Cyber ranges can recreate complex networks including both traditional IP interfaces and non-IP interfaces such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) hardware, software defined radios, and military standard data buses (Ten, Liu, & Manimaran, 2008). Consequently, the use of a cyber-range to recreate the operational environment limits the restriction on rules of engagement. Without the fear of damaging operational equipment, teams are free to emulate a full range of offensive and defensive TTPs. The affordances this represents is the ability to develop new TTPs and to refine and validate existing TTPs as a team. Although the aforementioned flexibilities and affordances do not receive much attention in CTF-focused literature, they are valuable considerations in the development of effective Red Team training. Additionally, their value in is the fact that they facilitate positive individual and team behaviors, engage and improve core cognitive capacities, support pedagogical and instructional design strategies, as well as, allow implementation of interdisciplinary approaches to modeling and simulation techniques that embraces concepts of engineering and human systems.

Figure 3

Offensive-Focus Cyber High Level Affordances and Attributes



Peer-to-Peer Mentoring, Motivation, and Engagement

The team aspect of CTF encourages members to engage in knowledge sharing and transfer often facilitated through peer-to-peer mentoring (Chen, 2013). In CTF challenges, lower skilled members learn from highly skilled members within a context rich training environment. Teaching by the highly skilled members reinforces learning, mitigates skill decay, and promotes the highest possible skill strength of the team. Scaffolding takes place in real-time by members in support of other members as well as in the CTF game-based challenges themselves. Leveraging game design elements such as role play/reversal, adjustments in challenge difficulty, point earning, and leader boards intrinsically motivates and engages members of varying skill levels. Additionally, game elements offer different ways to model and simulate authentic and artificial hands-on experiences requiring total team engagement.

Cyber security CTF enables the ability to model authentic and artificial system use cases and simulate current threats and attacks. Simulating current cyber threats and attacks supports training relevance and operational realism (Nagarajan, Allbeck, Sood, & Janssen, 2012; Shiravi, Shiravi, Tavallaee, & Ghorbani, 2012). Modeling system use cases through authentic or artificial means enhances a trainee's KSA by requiring critical and flexible thinking, exposure to familiar and new adversarial TTPs, and demonstration of skill in a dynamic training environment. Because the mapping of flags to relevant apprentice, journeymen, and master level KSAs is possible, highly skilled members sustain current knowledge states.

On the other hand, lower skilled members gain new knowledge through real-time feedback while engaged in challenges of increased difficulty. Thus, existing and emerging KSAs are leveraged and augmented. Enhanced KSA states are advantageous to quality of job performance in the operating environment (Schab, 2017). The cyber T&E operating environment requires teams to think fast, switch between concepts, and think critically about multiple concepts at the same time. For DoD systems, networks, and infrastructures, these cognitive capacities are vital in ensuring a system's survivability and operational resilience posture with respect to security controls implementation (CSTE Guidebook, Version 2.0, 2020).

Cognitive Flexibility, Cognitive Control, and Task Switching

As advancements in interconnectivity, automation, and data capture increase, adversary TTPs evolve and attack sophistication levels increase. This drives the importance for implementing cyber T&E Red Team training that targets the utilization and improvement of core cognitive capacities. Cyber security CTF challenges that require a shift between elements of a larger problem in an effort to solve it means team members will have to (a) integrate new TTPs, (b) simplify the problem, or (c) determine how smaller elements contribute to the larger problem (Spiro, 1988; Spiro, et al., 1987). As an example, placing "Easter eggs" within the solution path can aid teams in understanding the larger problem in order to revise and rapidly employ TTPs to capture the correct flag. In this context, Easter eggs serve as auxiliary flags (non-core) flags that do not result in point deduction and may contain useful data (such as part of a network diagram).

The Easter eggs can also help teams to avoid error by providing an opportunity to reframe from automatic response behaviors and engage working memory. In turn, they can reduce uncertainty in decision-making at various levels of problem solving and direct attention to the most relevant pieces of information (in the game and in memory) (Abrahamse, Braem, Notebaert, & Verguts, 2016; Braver, Gray, & Burgess, 2007). The switch of attention from the larger problem to the information the Easter egg aids in solving the larger problem and facilitates thought stopping through much deeper analysis of all pieces of information (Friedman & Miyake, 2017). By supporting executive function and control, cyber security CTFs assist team members (at the individual and team level) in advancing in the ability to adapt to newly encountered experiences with flexibility.

Game-Based Learning (GBL)

Improved cognitive capacities happen through three types of learning strategies including game-based, problem-based, and team-based learning. First, cyber-based CTFs utilize gaming principles often found in game-based training and applies them to real-world settings. Teams engage in competitive challenges that increase in difficulty after the capture of a flag. Correct capture of core flags, results in teams earning points. The earning of points and the real-time scoreboard enhances rivalry between teams and motivates teams (at the individual and team level) to perform well. Designed around a story, teams are role players in the game solving mission-based challenges. The narrative and mission-oriented elements give purpose and enrich the role players' immersive experience. As previously discussed, there are gameplay elements that encourage various types of thinking and competition driven mentoring (Hendrix, Al-Sherbaz, & Bloom, 2016; Alotaibi, Furnell, Stengel, L., & Papadaki, 2016).

A cyber security CTF where gameplay is unstructured permitting teams to capture flags in any order and by any means within the allowable rules of engagement encourages divergent and creative thinking. Real-time scoreboard feedback can rally team members and improve team cohesion. The guidance more experienced team players provide to less experienced role players supports transfer and sharing of knowledge. This can assist in improvement of player TTPs. Given that role players must often engage in several attempts to capture a flag, deeper levels of teamwork is encouraged among the role players. This cooperative gameplay mirrors behaviors Blue Team and Red Teams demonstrate in the operating environment.

Furthermore, the goal to catch the correct flag is exciting to teams. After the capture of a flag, team members often cheer and run around high fiving one another with a great deal of excitement. This is an expression of the fun element of game-based learning. Cybersecurity CTFs can achieve eliciting "excitement" and "motivation" during gameplay. It is important that designers develop challenges that motivate and excite the players to continue until the end. In this way, the full range of targeted KSAs receive attention from the players on a team.

Problem-Based Learning (PBL)

In the CTF environment, learning is hands-on rather than a didactic presentation of content for purposes of memorization. This is an essential component of problem-based learning (PBL). Moreover, per alignment with Bloom's Taxonomy (Krathwohl & Anderson, 2009), role players in the CTF environment can engage in mission challenges that require the use of higher-order thinking skills to solve a unique set of challenges. Role players evaluate the challenges set before them, analyze approaches, and apply the KSA strengths of each role player within the team to solve a problem rapidly and with minimal error. Since challenges are akin to aspects of the current threat landscape, there is authenticity in the process-oriented (collaborative) environment in which Red Teams operate. The ill-

structured problems presented within the CTF environment elicits inquiry-based thought among the team's role players. Consequently, the CTF training model is participant centered in design and in implementation (Yew & Goh, 2016; Hung, 2016; Hung, 2009; Hung, Jonassen, & Liu, 2008).

Team Based Learning(TBL)

As has been mentioned, CTFs are team-based competitions. Depending on design, the team's ability to solve challenges in any order they deem most appropriate given team makeup (strengths and weaknesses) affords autonomy. Additionally, it puts participants in the front seat of their learning and training experience as they are responsible for (1) how they prepare for competitions, (2) how they develop their team, (3) how long they engage in the CTF over the course of the multi-day experience, and (4) how they set team priorities (before/during gameplay). With this high level of autonomy, there are team-based learning (TBL) components that require consideration (Michaelsen & Sweet, 2008). First, development of a team of members that remains stable across competitions supports team permanency. Second, problem oriented challenges rather than direct instruction promotes divergent thinking during problem-solving process. Third, problems of high complexity require members on a team to decide which provided or home-developed hacking tool is best fit to capture the correct flag.

The TBL and PBL attributes of CTF makes it a feasible option for incorporation into academic and training programs. TBL offers the ability to scale the level of effort of the development team. Before/during an active competition, the development team is able to focus on operations and mission development rather than team preparation and designated functions of each team member. The latter is restricted to the teams themselves. TBL and PBL are both effective pedagogical strategies to employ in training complex, ill-structured concepts often present in cybersecurity (Davidson & Major, 2014). Although TBL and PBL share the before mentioned benefit, there are differences in each method.

TBL requires a bit more of a structured approach to its process and application of data from the instructor stance. Whereas in PBL, the instructor role is restricted to identifying the problem to be solved by the learner or trainee. TBL is more traditional in application than PBL without the requirement to alter the education or training program's outcomes and overall curriculum (Michaelsen, Davidson, & Major, 2014). Better stated, TBL has a greater degree of plug-and-play than PBL when incorporating their respective concepts and principles to content within an education or training program. Therefore, it is more efficient to invest time in mission challenge creation by reducing the development team role in TBL functions.

Instructional Design, Modeling, and Simulation

The critical thinking, creative use of TTPs and problem-solving experiences are opportunities for addressing the breadth and depth of relevant KSAs. By mapping the attack sequence for capturing a flag back to established cyber T&E to apprentice, journeyman, and master level KSAs, it ensures that capturing a flag is not simply game play. Rather, the attack sequence associated with capturing a flag links to cyber T&E relevant KSAs. Therefore, the skills practiced during an event is operationally relevant (Bomer, 1988; Tennyson & Rasch, 1988). Mapping back the attack sequence to approved and validated KSAs allows for the assessment of specific knowledge, comprehension, and performance objectives. In addition, mapping the attack sequence back to these KSAs helps determine whether the trainee met the performance objectives and at what proficiency level. Equally, capturing a flag allows trainees to demonstrate understanding of concepts required to extract a flag. In comparison to paper-based assessment, demonstration of understanding by performing the task is a better indicator of proficiency. Subsequently, by CTFs providing experiential exposure (Kolb, Boyatzis, & Mainemelis, 2001) to relevant problem sets, it enables the CTF model to improve Red Team readiness.

Likewise, the capacity to model the actual operational environment means it is plausible to address an array of cyber T&E competency and skill requirements. This may include modeling complex attacks such as nation state supply chain injection, all the way down to weak or default passwords. In addition, this can also include modeling difficult concepts such as reverse engineering, forensics analysis, and attack attribution (Kuhl, Sudit, Kistner, & Costantini, 2007). However, modeling these attacks is often limited by time constraints and enterprise IT systems (representative of operational environment). That stated the GBL aspect of CTF allows designers to pre-stage time-consuming tasks such as deployed exploit or insider threat operative. GBL in CTF can focus training as well as overcome known modeling and simulation limitations.

Simulated gaming elements, such as the back-story, aids in focusing training on relevant KSAs. Despite some artificiality, it presents role players training on relevant cyber T&E topics in a timely manner (i.e. adversarial assessment). To address the limitations concerning modeling attacks around only replicated enterprise IT systems, designers can develop flag concepts around the systems (and sub-systems) that are relevant to critical infrastructure such as Supervisory Control and Data Acquisition (SCADA) control systems (Ten, Liu, & Manimaran, 2008). In addition, designers can model attacks around artificial weapons systems in an offensive Red Team focused CTF.

DISCUSSION/CONCLUSION

This paper focuses on the benefits of offensive-focused Cybersecurity Capture-the-Flag (CTF). More specifically, how the affordances and attributes of the method can address gaps in current training to augment Red Team readiness. Thus, postulating that CTF is a useful paradigm to support DoD Cybersecurity Red Teams in maintaining high levels of readiness against the ever-evolving tactics, techniques, and procedures (TTPs) deployed by the adversary. With expansion in interconnectivity, automation, data collection, and analytic methodologies, government, industry, and academia have access to computerized capabilities to enhance productive efficiency. These efficiencies can span across processes, programs, and products. For example, the ability to speed up administrative processes through use of automation. For the DoD specifically, technology advancements enables greater connectivity between systems and networks enhancing warfighting capabilities. For instance, weapons systems (through engineering) can operate at deeper levels of integration and interoperability across systems, networks, and platforms. Thereby, strengthening fighting power and expanding the DoD's competitive edge over its adversary. However, increased technological capabilities present new challenges and barriers to weapons systems cybersecurity.

Additionally, technological advances and DoD enhanced software dependencies extends the adversarial attack surface on weapons systems and networks. Moreover, the adversary has the ability to develop and deploy anonymous, stealthy, and sophisticated attacks on these software dependent systems and networks in a rapid and agile manner. Attacks of this nature threaten weapons systems survivability and operational resiliency. Therefore, DoD senior leaders have an explicit dependency on cybersecurity test and evaluation (T&E Red Teams to mitigate risks to weapons systems, operational networks, and critical data infrastructures. Red Teams function as a collective unit as part of cyber T&E. They are accredited, certified and authorized to portray adversarial TTPs on DoD systems and networks. They emulate potential adversarial attack and exploitation methods against a system's current cybersecurity posture. These efforts help to improve an enterprise's Information Technology (IT) cybersecurity posture and Blue Team defense TTPs in an operational environment. As a mission essential resource to system survivability and operational resiliency, as well as an essential entity within the cybersecurity workforce, there is a need for this skillset. As such, Red Teams have specific training needs. Unfortunately, DoD Red Teams face a myriad of personnel, education, and training challenges. These challenges are typically associated with lack of personnel to fill the full range of cybersecurity demands due to rotational assignments, turnover, and attrition rates. Challenges also result from gaps in educational preparation and training practice, difficulties in scheduling time to train, and the inadequacy of traditional models of training. As a result, Red Teams readiness levels are impaired.

CTF team-based competitions offers a variable set of behavioral, cognitive, and pedagogical benefits, as well as a method, ideal for applying simple to complex modeling and simulation techniques. Traditionally, CTFs were an indoor/outdoor game engaging physical endurance, stealth, strategy, and observation. Today, due to computerized capabilities, the method is, in variable formats and styles, used across government, industry, and academia to educate or train cybersecurity concepts and skills. However, it is neither a formal method of training nor a required component in educational curriculum. Despite its current stance in government, industry, or academic education and training, there exists certain innate attributes and by design, affordances to CTF. CTFs, by design, promotes utilization and augments current core cognitive capacities such as flexibility, adaptability, and control. These design attributes, leveraged appropriately via hands-on competitive problem-solving challenges, augment these capabilities in Red Teams. When engaged in a CTF competition, behaviors such as knowledge sharing and transfer occur via peer-to-peer mentoring. Careful design of increasingly more difficult challenges that facilitates creative thinking and diversity of thought activates certain core aspects of cognition (e.g. thinking flexibly or deep problem analysis). Careful design also affords the ability to apply prescriptive instructional design methods and employ various modeling and simulation techniques to decrease or increase game fidelity.

During a CTF game-based competition, lower skilled players receive immediate and real-time feedback from higher skilled players. This encourages knowledge sharing and transfer among the team members. The occurrence of these

behaviors is difficult (and degraded) in Red Team operational test environments due to attrition, turnover, and rotational assignments. Consequently, the challenges included in a CTF needs to engage players at the personal (each team member), organizational (the whole team), and situational (complexity of each flag level). In addition, observation of the TTPs used by higher skilled players intrinsically motivates lowered skilled players to perform well. The point earning and associated community bragging rights are external motivators that contribute to the member's intrinsic motivation to acquire deeper knowledge, skills, and abilities for application in the operating environment. The unstructured format of a CTF is where creative and divergent thinking thrives. The setting allows teams to utilize team selected TTPs within the established rules of engagement. Teams are able to validate effectiveness of the TTP, refine various aspects of their applied TTP, and even develop new TTPs given resulting outcomes. Impacts on quality and depth of desirable behaviors relates to the size of the team, proximity of members, and diversity of skillset among team members.

Participation in a cybersecurity CTF promotes the use of core cognitive capacities such as flexibility, control, and task switching. Challenges requiring a shift between larger problem elements in an effort to solve it means team members have to (a) integrate new TTPs, (b) simplify the problem, or (c) determine how smaller elements contribute to solving the larger problem. The placement of Easter eggs within or adjacent to the solution path can aid teams in understanding the larger problem in order to revise and rapidly employ effective TTPs to capture the core flag and earn the largest amount of points possible. The nominal, undocumented Easter eggs (data files) supports flexible thinking and control over thinking to ensure focus is on the most relevant aspects of a larger problem set. Designers of the CTF must avoid applying penalty due to the discovery of an Easter egg. For example, when a team discovers an Easter egg, rather than resulting in a loss of points, these auxiliary flags can be used to support executive functions (i.e. thought stopping) or serve as motivating factor within the game.

Since a cybersecurity CTF is game based, designers can employ various elements of game play. These elements includes the use of the narrative (story), rules, goals, interaction, feedback, integration of elements, and fun. For instance, the story can enhance the immersive experience by ensuring scenarios represents information or request for action representative of the operational environment. Designers should determine ways to balance the use of the various game based elements employed when developing the CTF challenges. For example, making sure not to include a large degree of unnecessary information in the narrative.

CTF affords the integration of game-based, problem-based, and team based learning and instructional design prescriptions. The CTF experience is not only hands-on, but calls on useful and essential behavioral and cognitive skills Red Teams display and benefit from in the operational environment. They help address the breadth and depth of relevant KSAs. Mapping the attack sequence to relevant operational KSAs supports sustainment of current, and acquisition of emerging, KSAs. In addition, mapping the attack sequence back to KSAs helps determine whether the trainee met the performance objective and at what proficiency level. The hands-on PBL nature of CTF supports demonstration of KSA rather than regurgitation of facts. In this way, it is a better measure of performance and provides useful data for making inferences regarding links between a priori or a posteriori correlations to end-of game performance. An offensive-focused CTF provides a way to supplement (extending the training surface) traditional models of required training. How to best measure performance of players on an individual and team level needs further exploration. The design team for an offensive-focused CTF should include instructional designers as well as human factors specialists to support the design and flow of challenges.

ACKNOWLEDGEMENTS

The authors very much appreciate the support, direction and guidance by the Office of the Under Secretary of Defense for Research and Engineering (OUSD R&E), Director Developmental Test, Evaluation and Assessments (DDTE&A), and the Test Resource Management Council in the support required to develop this paper. The authors would also like to thank all additional parties for any review and suggestions toward improving paper quality.

REFERENCES

Abrahamse, E., Braem, S., Notebaert, W., & Verguts, T. (2016). Grounding cognitive control in associative learning. *Psychological Bulletin*, *142*(7), 693-728.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. *International Journal of Information Security, 6(2)*, 660-666.

Bonner, J. (1988). Implications of cognitive theory for instructional design: Revisited. *ECTJ*, *36*(1), 3-14.

Braver, T. S., Gray, J. R., & Burgess, G. C. (2007). Explaining the many varieties of working memory variation: Dual mechanisms of cognitive control. *Variation in working memory*, *75*, 106.

Chen, Y. C. (2013). Effect of reverse mentoring on traditional mentoring functions. *Leadership and Management in Engineering*, *13*(3), 199-208.

Chain, K., Kuo, C. C., Liu, I. H., Li, J. S., & Yang, C. S. (2018, April). Design and implement of capture the flag based on cloud offense and defense platform. In *2018 IEEE International Conference on Applied System Invention (ICASI)*, 686-689.

Chothia, T., & Novakovic, C. (2015). An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. In *2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*.

Davis, A., Leek, T., Zhivich, M., Gwinnup, K., & Leonard, W. (2014). The Fun and Future of CTF. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

Davis, M. A. (2020). Learning Geography through Mobile Gaming. *Handbook of the Changing World Language Map*, 3619-3631.

Defense Acquisition University. (2017, February 26). Test and Evaluation [Chapter 8]. In Defense Acquisition Guidebook.https://www.dau.edu/guidebooks/_layouts/15/WopiFrame.aspx?sourcedoc=/guidebooks/Shared%20Documents/Chapter%208%20Test%20and%20Evaluation.pdf&action=default

Defense Acquisition University. (2018, September). Cybersecurity and the Acquisition Life Cycle Interactive Tool (Power Point Presentation). https://slideplayer.com/slide/142456

Department of Defense Inspector General (2020, March 13). Follow-up audit on corrective actions taken by DoD components in response to DoD Cyber Red Team-Identified Vulnerabilities and Additional Challenges Facing DoD Cyber Red Team Missions (DODIG-2020-067). https://www.dodig.mil/reports.html/Article/2114391/followup-audit-on-corrective-actions-taken-by-dod-components-in-response-to-dod/

Department of Defense. (2020, February 10). Cybersecurity Test and Evaluation Guidebook [Version 2.0, Change 1]. https://www.dau.edu/cop/test/DAU%20Sponsored%20Documents/Cybersecurity-Test-and-Evaluation-Guidebook-Version2-change-1.pdf

EY. (2020). How does security evolve from bolted on to built in? https://www.ey.com/Publication/vwLUAssets/2020_GISS_pdf/$FILE/ey-global-information-security-survey-2020-report.pdf

Feng, W. C. (2015). A Scaffolded, Metamorphic {CTF} for Reverse Engineering. In *2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*.

Ford, V., Siraj, A., Haynes, A., & Brown, E. (2017, March). Capture the flag unplugged: an offline cyber competition. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*, 225-230).

Friedman, N. P., & Miyake, A. (2017). Unity and diversity of executive functions: Individual differences as a window on cognitive structure. *Cortex*, *86*, 186-204.

Government Accountability Office. (2018, October 9). Weapons systems cybersecurity. DoD just beginning to grapple with scale of vulnerabilities [GAO-19-128]. . https://www.gao.gov/products/GAO-19-128

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game Based Cyber Security Training: are Serious Games suitable for cyber security training?. *International Journal of Serious Games*, *3*(1). https://doi.org/10.17083/ijsg.v3i1.107

Huang, H., Ding, J., Zhang, W., & Tomlin, C. J. (2011, May). A differential game approach to planning in adversarial scenarios: A case study on capture-the-flag. In *2011 IEEE International Conference on Robotics and Automation*, 1451-1456.

Hung, W., Jonassen, D. H., & Liu, R. (2008). Problem-based learning. *Handbook of research on educational communications and technology*, *3(1)*, 485-506.

Hung, W. (2009). The 9-step problem design process for problem-based learning: Application of the 3C3R model. *Educational Research Review*, *4(2)*, 118-141.

Hung, W. (2016). All PBL starts here: The problem. *Interdisciplinary Journal of problem-based learning*, *10*(2), 2.

Krathwohl, D. R., & Anderson, L. W. (2009). *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*. Longman.

Kolb, D. A., Boyatzis, R. E., & Mainemelis, C. (2001). Experiential learning theory: Previous research and new directions. *Perspectives on thinking, learning, and cognitive styles*, *1*(8), 227-247.

Kuhl, M. E., Sudit, M., Kistner, J., & Costantini, K. (2007, December). Cyber-attack modeling and simulation for network security analysis. In *2007 Winter Simulation Conference*, 1180-1188.

McDaniel, L., Talvi, E., & Hay, B. (2016, January). Capture the flag as cyber security introduction. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 5479-5486.

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012, May). Exploring game design for cybersecurity training. In *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, 256-262.

Namin, A. S., Aguirre-Muñoz, Z., & Jones, K. S. (2016). Teaching cyber security through competition: An experience report about a participatory training workshop. In *International Conference on Computer Science Education Innovation & Technology (CSEIT). Proceedings* (p. 98). Global Science and Technology Forum.

NAVAIR University. (2015). Introduction to Cyber Warfare [Course # CISL-CYB-100-004]. www.navair.navy.mil

Panini, P. (2016). Red Teams vs. blue teams [Image]. Retrieved from https://securityaffairs.co/wordpress/49624/hacking/cyber-red-team-blue-team.html/attachment/red-team-vs-blue-team

Pricewaterhouse Coopers. (2018, July 22). The Global State of Information Security Survey 2018. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

Radcliffe, J. (2007). Capture the flag for education and mentoring: A case study on the use of competitive games in computer security training. *SANS Institute. http://www.sans.org/reading-room/whitepapers/casestudies/capture-flag-education-mentoring-33018*.

Schab, J. (2017). Tackling DoD Cyber Red Teams deficiencies through systems engineering [Thesis SANS Institute of Technology], SANS Institute of Technology Reading Room. https://www.sans.org/reading-room/whitepapers/testing/tackling-dod-cyber-red-team-deficiencies-systems-engineering-38020

Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *Computers & Security*, *31*, 357-374.

Spiro, R. J. (1988). Cognitive flexibility theory: Advanced knowledge acquisition in ill-structured domains. *Center for the Study of Reading Technical Report; no. 441*.

Spiro, R. J., Vispoel, W. P., Schmitz, J. G., Samarapungavan, A., Boerger, A. E., Britton, B. K., & Glynn, S. M. (1987). Cognitive flexibility and transfer in complex content domains. *Executive control processes in reading*, 177-199.

Strickland, A. (2020, June 1). NASA astronauts capture the flag on the space station and look ahead after historic launch. CNN. https://www.cnn.com/2020/06/01/us/nasa-astronauts-cassidy-behnken-hurley-iss-interview-scn/index.html

Spiro, R. J. (1988). Cognitive flexibility theory: Advanced knowledge acquisition in ill-structured domains. *Center for the Study of Reading Technical Report; [Report # .441].*

Spiro, R. J., Vispoel, W. P., Schmitz, J. G., Samarapungavan, A., Boerger, A. E., Britton, B. K., & Glynn, S. M. (1987). Cognitive flexibility and transfer in complex content domains. *Executive control processes in reading*, 177-199.

Schab, J. (2017). Tackling DoD Cyber Red Teams deficiencies through systems engineering.

SANS Institute Information Security Reading Room https://www.sans.org/reading-room/whitepapers/testing/tackling-dod-cyber-red-team-deficiencies-systems-engineering-38020

Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, *23*, 1836-1846.

Tennyson, R. D., & Rasch, M. (1988). Linking cognitive learning theory to instructional prescriptions. *Instructional Science*, *17*, 369-385.