Cyber Red Zone: Capture-the-Flag the DoD Way!

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

ABSTRACT

Cyber Red Zone (CRZ) is the U.S. Department of Defense's (DoD) multiday cybersecurity competition. These team-oriented cybersecurity competitions are open to government personnel across multiple technical career fields to learn or sharpen their tactics, techniques, and procedures (TTPs) in protection of defense networks, critical data infrastructures, and defense weapons systems (and subsystems) within a realistic, game-based environment. Now in its sixth iteration, design, and development of CRZ events utilize a specific formula that targets actual defense cybersecurity knowledge, skills, and abilities (KSAs) at three levels: apprentice, journeyman, and master. Typically, there are three flags per KSA targeted. Moreover, CRZ cybersecurity competitions take place over a 48-hour period. This two-day period allows for chained attacks, as well as participation from red teams and cyber protection teams. To maintain participant attention and sustain morale, ten Easter eggs hidden in the networked environment serve as a means of frustration reduction in the capture of high complexity flags without negatively affecting a team's overall score. In addition to the strategic placement of Easter eggs, teams can request point-reducing hints in order to facilitate learning of new TTPs. The intentionally chosen flags and strategic placement of Easter eggs ensures adequate coverage of key KSAs are being addressed, and that less experienced cyber teams can gain experience while still challenging the more experienced certified and accredited DoD Red Teams. Encompassed within a back-story and scenario-based missions representative of the current threat landscape, CRZ has garnered DoD senior leadership support and increased participation from DoD cybersecurity, Information Technology (IT), and engineering professionals. This paper will discuss the CRZ formula.

ABOUT THE AUTHORS

Ms. Tashara Cooper is a research psychologist for the Naval Air Warfare Center Training Systems Division (NAWCTSD). She has a master's in Instructional Design and Technology (Instructional Systems Design focus), as well as a Graduate Certificate in the Cognitive Sciences from the University of Central Florida. She is currently pursuing a master's in Modeling and Simulation (Human Systems focus). Her areas of interest include training effectiveness evaluation, flexible course/instructional design, supportive human performance technology development, and modeling and simulation. She has supported basic and applied research in intelligent tutoring, adaptive training, culture and trust, and intuitive decision-making. Currently, she leads a technology transition focused on data transport methods in simulation, supports the Office of Naval Research (ONR) Human Performance Training and Evaluation initiatives, integration of mixed reality (XR) innovative training solutions for aviators and aviator support personnel, cybersecurity courseware development, and Capture-the-Flag cybersecurity competitions.

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 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 Complex (NCRC) capture the flag exercises, and Navy Continuous Training Environment's Digital Radio Management System (DRMS).

INTRODUCTION

Every day in the news, an organization reports being hacked. In 2021, there was a ransomware attack every 11 seconds and that is only a fraction of the total cyber-attacks for the year. "Cybersecurity is the art of protecting networks, devices, and data from unlawful access or criminal use and the practice of guaranteeing confidentiality, integrity, and availability of information" (Cybersecurity & Infrastructure Security Agency, 2021). Governments and Corporations alike are struggling to keep up with the cybersecurity skills shortage in the workforce to combat the rise in cyber-crime. Demand is outpacing supply of qualified cybersecurity professionals (Center for Strategic and International Studies, 2016). Additionally, the pace of change in the cybersecurity industry requires constant training on the latest attacks. In addition to traditional training methodologies, creative game based approaches to training cyber-attacks are proving to be an effective way to train new skills.

This paper will focus on the cybersecurity training paradigm used in the National Cyber Range's (NCR) Cyber Red Zone (CRZ) Capture-the-Flag (CTF). Cybersecurity is a critical component of information and network security from both a functional and operational perspective. With advances in computerized tools and technologies, the threat landscape for cyber-attacks are constantly changing and the impacts of a data breach are so devastating to organizations and their reputation, training the cybersecurity workforce is a top priority for these enterprises. Institutions and organizations are leveraging the structure and architecture of gaming to supplement cybersecurity and information assurance related educational and training needs. NCR's CRZ annual event hosted in Orlando, Florida takes place across multiple days. Distributed self-formed teams across multiple geographic areas engage in discovering and exploiting vulnerabilities placed within the gameplay environment. This paper will discuss CRZ's flag design approach, factors driving the CRZ model, and game design methodology. In addition, discuss the benefits of CRZ as compared to other cybersecurity events.

Non-Military Cybersecurity Events

Individual or team-based cyber defense contests and competitions are being utilized as an educational strategy or training paradigm across K-12 education, post-secondary academia, industry, and government/military. For example, at the K-12 level, the Air Force Association (AFA) established Cyber Patriot program. Cyber Patriot is a National Youth Cyber Program, which hosts one of the largest cyber defense competitions nationally and internationally. Event name varies based on geographic area where event takes place. Cyber Patriot is designed for high school and middle school students (Air Force Association, 2013). Students oversee securing virtual networks within a fast-paced, high stakes, realistic simulation. This allows students to get hands on experience in defending a system on both Windows and Linux operating systems within scenarios focused on hardening and removing vulnerabilities. The goal of Cyber Patriot is to increase student interest in cybersecurity to meet the needs of an increasingly technical workforce.

At the post-secondary level, there is the National Collegiate Cyber Defense Competition (NCCDC). The major mission of this competition is to supply institutions with a controlled environment to assess student conceptual and operational knowledge, skills, and level of competency in protecting computer information and network infrastructures. The basis of assessment is the institution's cybersecurity-oriented curriculum. In other words, the NCCDC provides the place for institutions to evaluate the effectiveness of its curriculum to aid students in meeting and managing the challenges of cybersecurity. By providing an operational environment to test against curriculum, students can practice against specifically trained TTPs.

Beyond events designed for individuals or teams at the K-12 and post-secondary level, there is DEFCON. DEFCON is the first cybersecurity focused conference to host a CTF event that attracts professionals across various technical fields. Currently, considered the elite hacking event, DEFCON encompasses both attack and defense style hacking challenges. Teams compete against each other, and the winning team earns the coveted DEFCON black badge. As mentioned with advances DEFCON and the rise of other CTF competitions have occurred on a global scale. These contests range from game and server hacking, taking ownership over other participant systems, or protection of a system or service. Upcoming DEFCON events will employ a more training centered model comprised of a multiday course of study carrying a certification. DEFCON events are open to participants inside and outside of the federal workforce. However, the federal government realizes the benefit of using game based methods such as CTFs for training. As a result, government and military organizations have begun to invest in the design, development, and deployment of CTF events.

One such event is the President's Cup Cybersecurity Competition that is open to the federal workforce. It is managed by Cybersecurity & Infrastructure Security Agency (CISA). This event provides real world scenarios in a game based fashion where teams, or individuals, apply technical skills to complete cybersecurity tasks at varying levels of complexity. All President's Cup challenges are mapped back to work roles from the National Initiative for Cybersecurity Education (NICE) framework. Mapping challenges to NICE standards moves this event beyond fun gameplay into valuable experiential training. While the stated examples share certain aspects that make them effective in meeting he goal of information and network security as defined in the exercises and scenarios for each event, information and network security is more complex and carries higher consequence from the weapons systems perspective. Thus, preservation and protection of such systems requires knowledge, skills, abilities, and other characteristics (KSAOs) as compared to preservation and protection of standard enterprise IT infrastructure. To that end, inadequately secured computerized military equipment and systems means a weakened military posture.

Military Cybersecurity Events

With realization of the benefit of experiential, gamed based training methods, like CTF, multiple Department of Defense (DoD) agencies have engaged their cyber security workforce in developing, hosting, and participating in cyber-based competitions. The cyber-based competitions differ in length, format, and participation level. For instance:

- single day or. multi-day
- attack, defend, Jeopardy-style, or mixed-mode (combination of Jeopardy-style with an attack or defend mode)
- individual or team-based

The Army Cyber Institute's (ACI) premier event is called All-Army CyberStakes CTF. In its fourth year, this event is an individual, online Jeopardy-style competition that is open to all federal employees and ROTC (cadets and attending service academies). The event tests a wide variety of skills related to forensics, cryptography, exploitation (binary and web-based), as well as reverse engineering (Army Cyber Institute, 2022). ACI provides guidance on how to integrate All-Army CyberStakes into an already established training curriculum. That said, it might present opportunities to be modified for team-oriented training. Another virtual CTF used by the Army is a modified version of Artemis (spaceship bridge simulator). In this game, teams must infiltrate and take control of other team's ships via computer networks, attack other teams, defend their own ships, and formulate solutions to mishaps (Hames, 2015).

Recently, the Marine Corps began working NCR to develop the Marine Corps Cyber Games (MCCG) event. It will be a defensive cyber operations focused event with emphasis on protecting hardware and software unique to the DoD. Additionally on the U.S. Marine Corps side of things, the Deputy Commandant for Information is in its third iteration of its CTF called Cyber Games. Cyber Games focuses on offensive cyber operations. Cyber Games is a team-based competition. Teams are comprised of six to ten Marines and civilian Marines of varying rank and can be geographically dispersed (Marines, 2022). Last iteration involved national (i.e., Maryland) and international (i.e., countries) and leveraged the NCR hosted CRZ environment built by scientists and engineers at the Naval Air Warfare Center Training Systems Division.

CYBER RED ZONE

CRZ is the NCR's annual offensive cyber operations DoD Red Team cyber-based CTF event. Although the focus is on DoD Red Team cyber offensive operations, other teams and technical members within the DoD benefit from participation in the event (e.g., Blue Teams, engineering, etc.). For instance, Blue Team members are exposed to various attack TTPs an adversary could use to gain access and exploit newly discovered vulnerabilities. Such exposure can potentially inform current and future defense TTPs Blue Team members employ against same or similar attacks experienced during the event. As a result, CRZ attracts a wide range of experts with limited to extensive experience engaging in cybersecurity or cyber security-based competitions. CRZ offers various flexibilities that several of the before mentioned events do not, such as team member location. Meaning, teams can be distributed across different military sites within various geographic areas, use of commercial or in-house developed tools, and use of equipment that is either CRZ provided equipment or participant owned equipment. Moreover, CRZ does not place limits on team member size. Through observation and self-reports, teams value this level of autonomy.

To participate in CRZ's 48-hour event, self-formed teams must register members and state any tools or hardware-in-the-loop they intend to utilize outside of what is offered as part of CRZ. In addition, each member must individually complete a demographic and pre-event questionnaire as a required component of registration. At the end of the event, participants are encouraged to complete a post-event questionnaire about their experience during the event. Completion of the post-event questionnaire offers teams the opportunity to earn additional points to ending score. These additional points are pre-designated, and are the same for all teams. However, to earn the post-event questionnaire must be fully complete. As part of the sixth iteration of the event, the authors as well as other key event planning personnel have been exploring ways to measure the construct of creativity in attack approaches. However, such is beyond the scope of this paper, and will be discussed in future publications post deployment and analysis of results.

The Range

CRZ's annual events are out of the NCR's complex in Orlando and is accessible to DoD teams remotely via global DoD networks. Teams can connect to the range from the Joint Mission Environment Test Capability (JMETC) and Multiple Independent Levels of Security (MILS) Network, also known as JMN. Alternatively, teams can connect to the range via the Joint Information Operations Range better known as the JIOR network. Both networks provide the same level of service and access into the range. In addition, teams that do not have access to JMN or JIOR have the option to play in person at the NCR complex in Orlando which hosts an array of testing events in support of understanding and mitigating cybersecurity risks for the DoD.

The Environment

CRZ CTF is architected to comprise three major components in support of gameplay: IT support systems, game support Virtual Machines (VMs), and the CTF game space. All teams have access to the game support (CTF event) VMs and hardware in the loop (HITL), IT support systems (admin) VMs (scoreboard, chat server, file share), and hosted attack VMs (Kali w/ additional installed open-source tools). See Figure 1 (VMs used to support gameplay for the teams diagram) and Figure 2 (architectural diagram of the VMs the teams are attacking).

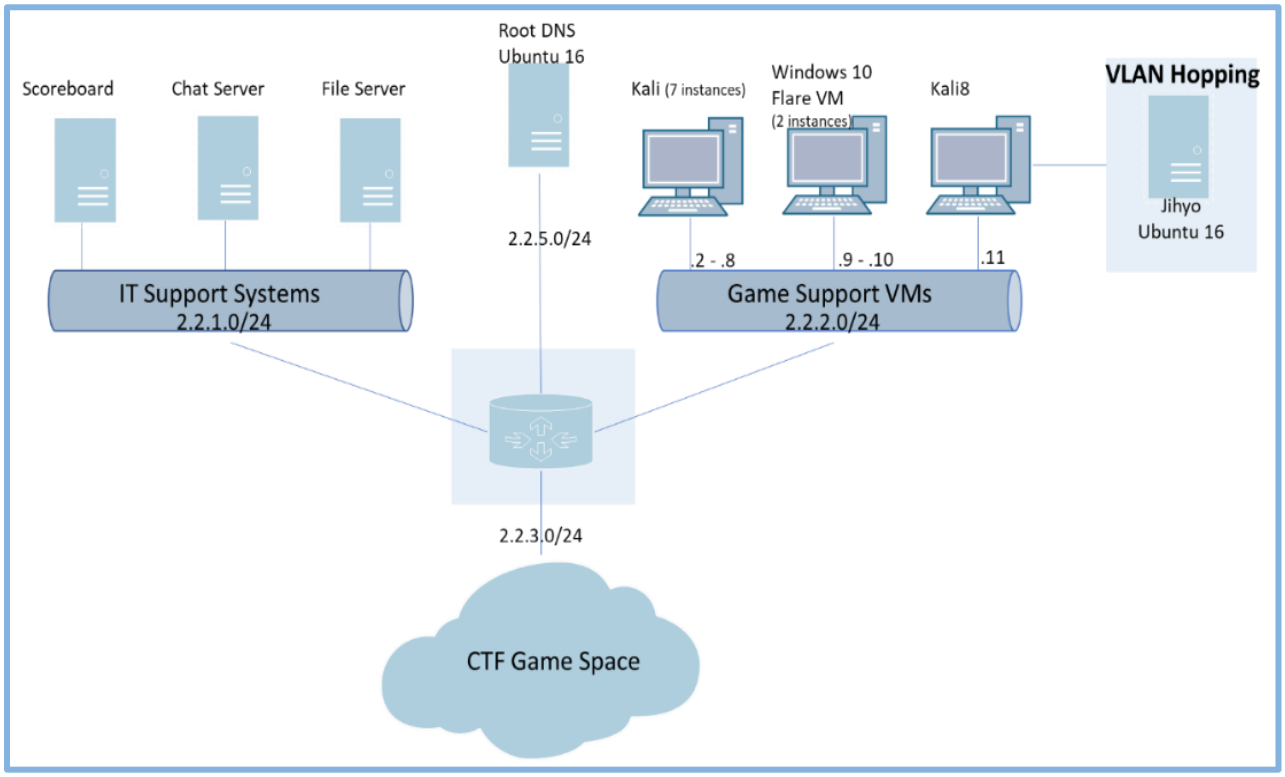

Figure 1. Diagram of the VMs Used to Support Gameplay for the Teams

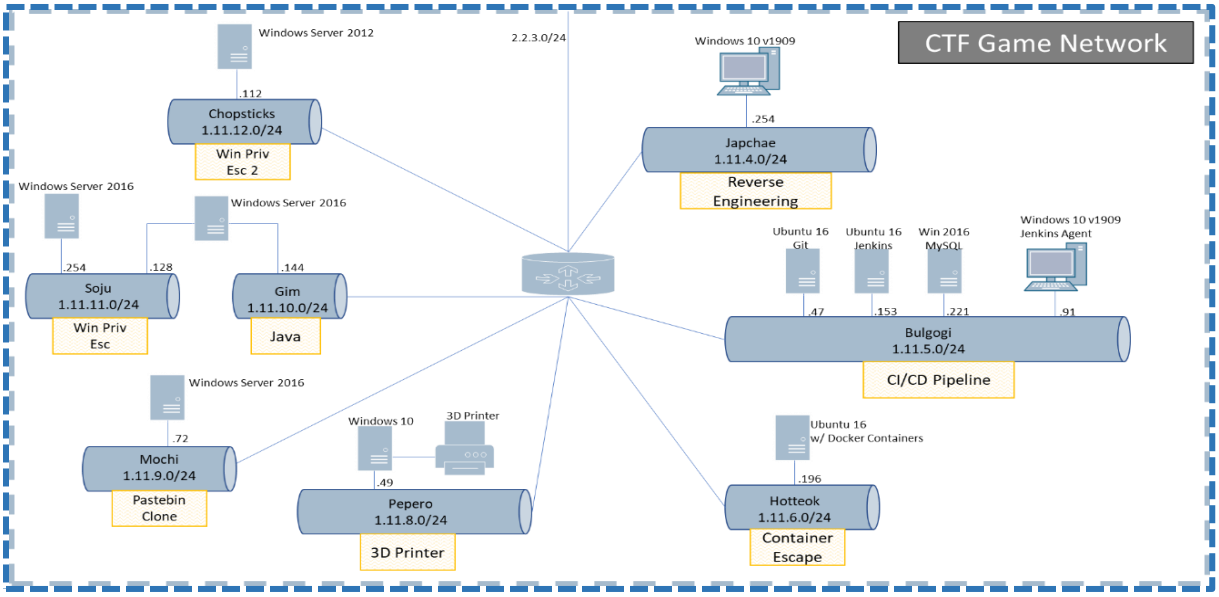

Figure 2. Architectural Diagram of the VMs the Teams are Attacking

The Teams

Typical CRZ events consist of over 30 DoD teams comprised of an average of four to ten members of variable skillset, age, and gender. These teams are individuals who are military, government civilians, or government contractors. Given teams are formed by the members themselves based mostly on the organization where they work, there are no restrictions on how many members make up a team; however, the majority consist of an average of four to ten people. Some organizations have enough members to host multiple teams in the event. Consequently, team member expertise varies within and across the formulated teams. Team members participate in CRZ via their JMN or JIOR node. If they are using the range provided systems, they use remote desktops to connect to VMs on the CRZ range in the game support VM. Teams with a larger number of people than provided attacking VMs must share their systems. If teams are providing their own attacking systems, they are connected logically to the game support VM. The distributed nature of teaming and team placement scoring (e.g., first, second, third, etc.) elicits somewhat of a team "bragging rights" element (Shi et al., 2021). Previous teams repeat participation and new teams are formed (or are reformed) based on the desire to improve on a previous score or out score certain teams for well-deserved "bragging rights." It has been our observation, as well as participant self-reporting, that "bragging rights" motivate the competitive nature of competing teams. As stated teams are distributed and geographically dispersed. However, it is important to note that this dispersion is within the United States (US), or from the US but stationed in places such as Japan.

CRZ FLAG DESIGN APPROACH

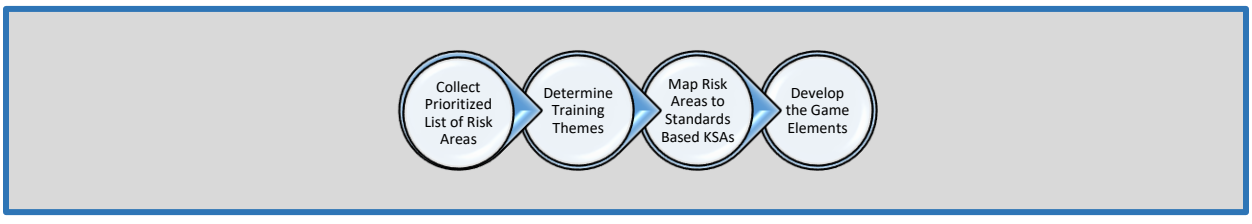

Figure 3. Flag Design Approach Flowchart

By design, all flags are designed to achieve the goal of meeting current training needs. Flags are also designed to be captured using freely available and open-source tools. All flags are designed with publically disclosed vulnerabilities. CRZ is unclassified (UNCLASS), and teams cannot use classified hardware, software, or TTPs during these event. To prepare the gamified CTF a lot of work goes into the flag design (See Figure 3) and challenges that each team will face. Because the cyber world moves at an incredible pace, it is important that CRZ events address the most relevant cyber threats, are data-driven, and mission impact-based (DoD, 2018). Therefore, the first phase of flag design involves procuring a new list of priorities to train. These priorities are obtained from a survey sent to senior leaders from the Developmental Test, Evaluation, and Assessments (DTE&A) cyber working group as well as other event stakeholders. This step ensures CRZ is training relevant and current cybersecurity risk areas specific to DoD systems. For the CRZ 2022 event, DoD proprietary protocols, supply chain, and additive manufacturing were high on the list of cyber risk areas. To address these risk areas, hardware is either procured or custom software is written by flag designers at the NCR complex in Orlando for the participants to practice their attack TTPs.

After identification of relevant risk areas, the next phase involves pulling in Cyber Security Evaluation Team (CSET) expertise at the NCR Orlando complex. CSET provides the CRZ team with flag themes. These themes are conceptual ways to address the stakeholder's risk areas. Armed with the risk areas and themes, the third phase involves the CRZ team generating flag ideas based on mapping risks areas with a baseline set of KSAs defined in the Development Test Cyber Vulnerability Analysis Standards (DT Cyber VA). The CRZ team selected the DT Cyber VA as the KSA reference document because it provides support in identifying KSAs that may be part of qualification standards at the organizational and analysis level. In addition, the document places emphasis on cybersecurity KSAs that are common across DoD components (or organizations within the components) that may contain their own specific guidance, processes, or procedures essential for altering DT Cyber VA standards through any additional qualification KSAs the organization or its components may need to train. Utilization of the DT Cyber VA document for mapping risk areas communicated by DoD senior leadership ensures that the event contains training relevant concepts against current cybersecurity risks and threat landscape (Callaghan, Savin-Baden, McShane, & Eguiluz, 2015).

The last phase of CRZ event design is to develop a compelling story line that ties the flags all together in a cohesive manner. This gamification element increase engagement because the flags are now challenges tied to an overall mission set with purpose and impact, as well as, learning (Landers & Landers, 2014). By adding an immersive story element, the flags now become part of a bigger mission to accomplish a higher-level purpose rather than simply completing a checklist. Since the CRZ event has teams with varying skill sets, the event is designed with three apprentice, three journeyman, and three master difficulty levels. In other words each flag is designed to map to only one level of difficulty. This reduces the barrier to entry for lower skilled teams while still allowing the advanced teams to be challenged. Additionally, teams with varying skill level can scaffold up less experienced members by assigning appropriate easier flags and having more experienced members demonstrate how they solve harder flags. This peer mentoring models how team CTF events train to the greatest common denominator.

THE CRZ FLAG DESIGN MODEL: CONSIDERATION FACTORS

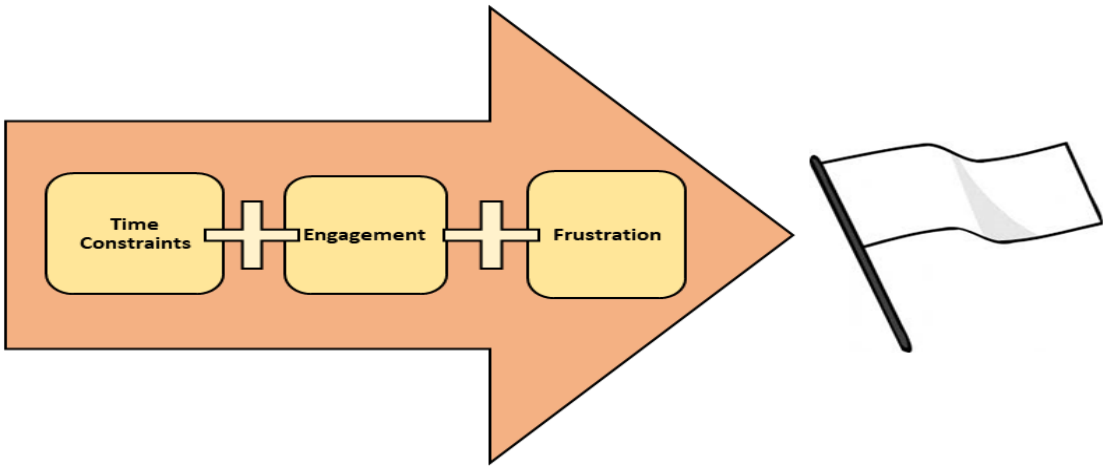

Figure 4. CRZ Model Design Considerations

Developmental, Operational, Test and Evaluation (DOT&E) KSA document outlines three categories of mastery (apprentice, journeyman, master). The model of nine flags with three at each skill level was derived using trial and error from past events and based on the DOT&E KSAs document. From past events, the primary factors considered for designing flags have been that of time constraints, engagement, and frustration levels (See Figure 4 above). Use of this flag design model ensures teams of all skill levels are challenged for the entire duration of their 48- hour session. That is, the design helps ensuing proper time is allocated to successfully capture the nine flags and complete game challenges. Moreover, it was observed that the inclusion of a realistic back story increases overall participant engagement. Lastly, in theory, the challenge hints provides opportunities (through scaffolding) to exchange points for reduced frustration (Caulkins, Marlowe, & Reardon, 2018).

More specifically, to increase individual and team engagement (recommendation from past user feedback surveys), CRZ added Easter eggs, source for additional points, in the environment. These are undocumented but helpful hints in the game. This encourages teams to better explore the environment and do additional reconnaissance when needing to step away for a minute from a difficult flag challenge. Throughout the environment there are vulnerabilities placed that are not part of the core mission scenario. If teams discover these undocumented vulnerabilities and exploit them, they unlock additional clues to help them with their core mission. For example, if a team exploits the captain's laptop, left in a trash can, the team could uncover network topology diagrams with needed IPs that are useful for the core mission. In CTFs, these ancillary missions are called Easter eggs. In addition to the help they provide, they also present an opportunity to task switch. Task switching postulates that moment-to-moment cognitive task performed, and the effectiveness of performance is a byproduct of multifaceted interplay of deliberate intention governed by goals and frequency and recency of alternative task afforded by the stimuli (Monsell, 2003). Thus, the step away is a cognitive benefit to teams during the problem solving process. Furthermore, this step away that Easter eggs provides to teams does not promote stopping or ending participation but promotes agile or adaptive thinking relative to TTP approach. Essentially, this gives teams a productive task to achieve while giving them a chance to regroup and come up with a divergent plan of attack by removing attention away from a complex task to a much simpler or more easily achievable (yet complex-task informative) one. While Easter eggs in the environment don't accomplish a core mission objective, they do help keep distractions focused on context relevant actions rather than frustrations leading to disengagement.

Lastly, to ensure teams of all skill levels are productive during the CRZ event, hints are available for a point deduction. Each of the nine primary flags (three apprentice, three journeymen, and three master) have various levels of hints, each with increasing levels of help and corresponding points deduction from their game scoreboard. If a team decides to take all the hints for a flag, then this will result in getting no points for that specific flag. However, teams will unlock a walkthrough video that provides them with the proper set of actions necessary to capture the flag. Some flags by the nature of the real world environment have multiple avenues for success. In such cases the flag designer presents only the primary way of capturing the flag. The walkthrough video, made by the flag designer, offers teams an opportunity to learn this new TTP by following along with the video and actually performing the necessary keystrokes. To collect performance metrics, the hosted kali VMs on the range are setup with a custom bash shell (i.e., Linux command prompt) logging script to collect timing information and the specifics of what the commands were that the team used to initiate an attack against a target. The modified bash history is then compared against successful capture of a flag.

Flag Submission Tracking

For CRZ events, the game scoreboard tracks flag submission. In addition, the scoreboard not also keeps track of incorrect guesses. This is achieved by using timing information from when a flag was obtained on the game scoreboard in relation to when the team started their attack via the bash logging script. Team performance can be assessed per flag, that is, if provided the flag is captured via command line attacks. While performance measures are important to investigate, it is also equally important to investigate how effective this event is at training. Specifically, how well it does at improving performance in the identified risk areas. Currently, this type of data is being captured at the reaction level via self-reports provided to team members. Each team is given a battery of surveys via the in-game file share before the event starts to assess pre-event knowledge and again after the event to see if the event helped improve understanding of the KSAs targeted by CRZ. The CRZ team is exploring other performance measurement and training effectiveness approaches for future iterations of the event that go beyond self-reporting, but that will not involve additional surveys to complete or interrupt the flow of problem-solving.

CONCLUSION

Various institutions and organizations employ computer security contests and competitions, such as capture-the-flag (CTF) to attract talent, retain talent, introduce cybersecurity topics, or train cybersecurity personnel. K-12 education, academia and even industry host or deploy such events. In recent years, the government and military have engaged in the design, development, and deployment of CTF cyber-based competitions. As a major focus of this paper, the National Cyber Range's Cyber Red Zone event built in collaboration with the Naval Air Warfare Center is increasing in popularity among DoD Red Teams and other member of the cybersecurity workforce.

DoD Red Teams are National Security Agency (NSA) certified, as well as, accredited by the United States Strategic Command with the primary role of conducting adversarial assessments (AA) on defense systems (subsystems) underlying networks and data infrastructures. Such personnel often participate in CRZ and can carry multiple forms of cyber centered certifications. In other words, these teams are critical technical assets, so it is important for these teams, and those supporting these types of teams, to continually learn and sharpen individual and collective skills associated with defense cybersecurity. DoD Red Teams focus on uncovering weapons systems security vulnerabilities that may exist within defense networks and data infrastructures. Moreover, DoD Red Teams help inform weapons systems program goals and strategic objectives.

Given adversarial cyber operations rapidly evolve as technology continually advances, defense missions and systems remain at risk from adversarial cyber operations. Therefore, it is the reason why the first phase of designing flags for CRZ events involves collecting data from senior leaders regarding current risk areas in defense cybersecurity. Obtaining information on relevant, current day risk areas ensures real-world applicability post the CRZ CTF competitive training experience. In its sixth iteration, CRZ flag design is a multi-phased approach as shown in Figure 3. As mentioned, consideration to factors such as timing, engagement, and frustration serves as a guidance model during flag and challenge design for the multi-day event as well as the integration of game elements (such as storyboard, Easter eggs, chat, etc.). Future publications aim to elaborate more on participant performance outcomes and qualitative feedback. In addition to providing an engaging and challenging training experience, CRZ provides opportunity for participants to think critically, as well as extend their current knowledge and skill base. For instance, use of Easter eggs provide opportunity to task switch when encountering high complexity flags. As well as hint-prompted walk-through videos provides opportunity to about more advanced TTPs.

Future iterations of CRZ should examine methods for determining to what degree CRZ elicits offensive and defensive creative unknown TTPS and the link between the use of those TTPs in the capture of specific flags or completion of particular challenges. In addition, answering the question, does CRZ flag challenges elicit creative attack approaches in participants? As well as additional methods for assessing training effectiveness of CRZ. With advances in technology, exploring ways to integrate automation of flag order and complexity across teams based on each team's performance, inclusion of mixed reality devices to enhance the immersive experience or investigate facets of attention or design of comparison experiments (i.e., CRZ versus other CTF training simulations) are areas worth exploration.

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

Air Force Association. (2013). What is Cyber Patriot? AFA CyberPatriot Website (uscyberpatriot.org)

Army Cyber Institute. (2022). All-Army CyberStakes Capture-the-Flag. ACI CTF

Callaghan, M., Savin-Baden, M., McShane, N., & Eguiluz, A. G. (2015). Mapping learning and game mechanics for serious games analysis in engineering education. *IEEE Transactions on Emerging Topics in Computing*, *5*(1), 77-83.

Caulkins, B., Marlowe, T., & Reardon, A. (2018, July). Cybersecurity Skills to Address Today's Threats. In *International Conference on Applied Human Factors and Ergonomics* (pp. 187-192). Springer, Cham.

Center for Strategic and International Studies. (2016). Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills.

Cybersecurity & Infrastructure Security Agency. (2021). *Cybersecurity Awareness Month 2021*. Retrieved from CISA: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Awareness%20Month%202021%20-%20Why%20is%20Cybersecurity%20Important.pdf

Department of Defense. (2018, April 25). Cybersecurity Test and Evaluation Guidebook Version 2.0. Cybersecurity Test and Evaluation Guidebook 2.0 (daytonaero.com)

Hames, J. (2015). Virtual capture-the-flag helps Soldiers enhance cyber capabilities. Virtual 'capture the flag' helps Soldiers enhance cyber capabilities | Article | The United States Army

Landers, R. N., & Landers, A. K. (2014). An empirical test of the theory of gamified learning: The effect of leaderboards on time-on-task and academic performance. *Simulation & Gaming*, *45*, 769-785.

Monsell, S. (2003). Task switching. *Trends in cognitive sciences*, *7*, 134-140.

Shi, X., Kavussanu, M., Cooke, A., McIntyre, D., & Ring, C. (2021). I'm worth more than you! Effects of reward interdependence on performance, cohesion, emotion, and effort during team competition. *Psychology of Sport and Exercise*, *55*, 101953.