Tailored Cybersecurity training in LVC environments

Denise Nicholson, Lauren Massey, Eric Ortiz and Ryan O'Grady
Soar Technology
Orlando, FL Ann Arbor, MI
denise.nicholson@soartech.com, lauren.massey@soartech.com, eric.ortiz@soartech.com, ryan.ogrady@soartech.com

ABSTRACT

Cyber vulnerabilities are continually emerging as a threat to our national and economic security and stability. Reports indicate a tremendous gap in skilled personnel capable of filling our growing need for a Cyber Security workforce to operate, analyze, protect, and defend our critical infrastructure systems. In response, the Department of Homeland Security has developed a national strategic program geared toward education, the National Initiative for Cybersecurity Careers and Studies (NICCS). This program has developed the National Cybersecurity Workforce Framework which "provides a blueprint to categorize, organize, and describe cybersecurity work into Specialty Areas, tasks, and knowledge, skills and abilities (KSAs)" (NICCS, 2015). There is a logical progression to turn to modeling and simulation-based training systems to provide experiential learning to augment the knowledge and skills being developed in classroom and e-learning cyber security certification and degree programs. By using a scenario-based approach in Live, Virtual and Constructive (LVC) simulation, trainees can practice higher order skills and have an opportunity to experience realistic stressors in dynamic situations. We will present concepts for use of on-going research into three different interactive cybersecurity training activities 1) a 3D gaming environment for Insider Threat training, 2) a virtual Cyber Security Instruction Environment (CYSTINE) for penetration testing with cognitive agent defenders and 3) the use of red-team verse blue-team, live simulation, exercises as realistic, challenging experiences for computer network defense. We will discuss these cyber learning experiences within a use case of a trainee progressing through a sequence of training tailored to his or her personal needs and objectives, such as envisioned within our early research on a project entitled *Fast Learning from Unlabeled Episodes for Next-generation Tailoring* (FLUENT) as part of Advanced Distributed Learning's (ADL) future Training and Learning Architecture (TLA).

ABOUT THE AUTHORS

Denise Nicholson, Ph.D., CMSP, is the Director of Soar Technology's new Technology Area "X" leading an effort to explore, identify and pursue innovative applications of intelligent systems for critical and challenging problems, such as Cyber Security. Dr. Nicholson has a Ph.D. and M.S. in Optical Sciences from the University of Arizona, and a B.S. in Electrical Computer Engineering from Clarkson University.

Lauren Massey is a graduate research assistant at Soar Technology currently supporting the FLUENT program under ADL sponsorship. Lauren is a Master's student in Software Engineering with an emphasis in Cyber Security at Embry – Riddle Aeronautical University, Daytona Beach, and received a B.S. in Human Factors and Psychology from Embry – Riddle Aeronautical University, Daytona Beach in 2014.

Eric Ortiz is Project Manager of Unreal Engine UE4 Support & Licensing at SoarTech, with over 20 years of experience in the development of digital media content, interactive web-based technologies, military simulations, serious games, and virtual environments (VE). Eric has extensive knowledge in 3D content applications and VE-related game engines. Eric is a Ph.D student in the University of Central Florida's M&S program and recently completed a graduate certificate program in the Foundations of Cybersecurity from the University of Maryland.

Ryan O'Grady is the technical lead for Soar Technology's emerging business area in cyberspace training and visualization and is a senior software engineer in the Intelligent Training business area. Mr. O'Grady received a BSE in Computer Science Engineering from the University of Michigan in 2004. Certifications: Security+, CPTE, OSCP.

Tailored Cybersecurity training in LVC environments

Denise Nicholson, Lauren Massey, Eric Ortiz and Ryan O'Grady
Soar Technology
Orlando, FL Ann Arbor, MI
denise.nicholson@soartech.com, lauren.massey@soartech.com, eric.ortiz@soartech.com, ryan.ogrady@soartech.com

INTRODUCTION

A Cybersecurity Workforce Need

The job market of cybersecurity is exploding; moreover, this market suffers from a severe workforce shortage. It is projected "that the cybersecurity workforce is expected to rise to 6 million (globally) by 2019, with a shortfall of 1.5 million jobs" (CSO, 2015). The exponential growth of cyber-attacks each year is overwhelming to the current state of the cyber workforce. Therefore, the Department of Homeland Security has developed a national strategic program geared toward education, the National Initiative for Cybersecurity Careers and Studies (NICCS). This program has developed the National Cybersecurity Workforce Framework which "provides a blueprint to categorize, organize, and describe cybersecurity work into Specialty Areas, tasks, and knowledge, skills and abilities (KSAs)" (NICCS, 2015). This blueprint serves an as interactive tool (see start-up menu options in Figure 1) that can inform current professionals, as well as those interested in joining the workforce, about opportunities and training to begin and/or advance cyber careers. Moreover, this tool outlines the educational requirements for a new generation of the cyber workforce while ensuring that established professionals maintain training in the latest trends in this field of ever-changing challenges.

Figure 1: NICCS Interactive Framework

A training catalog is also provided as an entity of the strategic program, in which interested parties can search for courses by specialty area, keywords, and proficiency levels. The search then identifies appropriate available online and in-person courses. Individuals are able to search the framework to discover which area of the cyber workforce is of particular interest, then investigate the training catalog that presents course options to achieve this endeavor.

Although a multitude of courses offered on the NICCS training catalog can identify the appropriate course for an individual based on specified information such as the learner's assumption of his or her level of expertise in a subject matter, the courses are not individualized to fit the learner's educational style or nor can they identify the learner's actual expertise level. The development of a training mechanism that is customizable to the trainee could accelerate the development of expertise and help manage the workforce shortage. The Department of Defense has recognized the need for modifiable learning capabilities across the spectrum, not just in the cyber security field, and have developed the Advance Distributed Learning (ADL) Initiative.

Advance Distributed Learning (ADL) Initiative

The Advanced Distributed Learning (ADL) initiative has a vision for a Personalized Assistant for Learning (PAL), which will help provide life-long, relevant, tailored, timely access to learning content and performance aids (Regan et al., 2013). This vision is accomplished through the setting of enhanced learning experiences which envelope the learner in a range of experiences that have been individualized to the user's situation through a training and learning architecture (TLA). As illustrated in Figure 2, the TLA encompasses four different aspects (Regan, 2013):

- *Learner profiles* provide basic information regarding the user such as current competencies and learning style.
- *Content Brokering* provides decision-making to set the type of content the user needs to complete to accomplish his or her unique cyber-driven goals, relative to the current competency levels and learning style provided in the learner profile.
- *Experience Tracking* allows for the learner profiles to be updated as the learner progresses in competencies in the cyber subject matter. This aspect can also be beneficial to managers who have assigned modules to track an individual's progress.
- *Competency Network* can be considered the library of course content that could be pulled by the content brokering feature for the learner.

Figure 2: Components of the TLA

While participating in the NICE working group, an opportunity was identified to leverage the NICCS framework and catalog of competencies as input to the TLA competency network to help drive selection and recommendations of experiences and courses for the learners. Moreover, having an automated PAL provide assistance to learners can help avoid inappropriate use of such a catalog of NICCS training in which users may attempt material that they are not prepared for, or the material may be presented in a manner that not beneficial to the learning environment. The creation of such an automated tailoring capability to drive the training experiences of a trainee progressing through a sequence of training tailored to their personal needs and objectives is envisioned within our early research on a project called FLUENT (Fast Learning from Unlabeled Episodes for Next-generation Tailoring) as part of the ADL's future Training and Learning Architecture (TLA).

EXAMPLE USE CASE

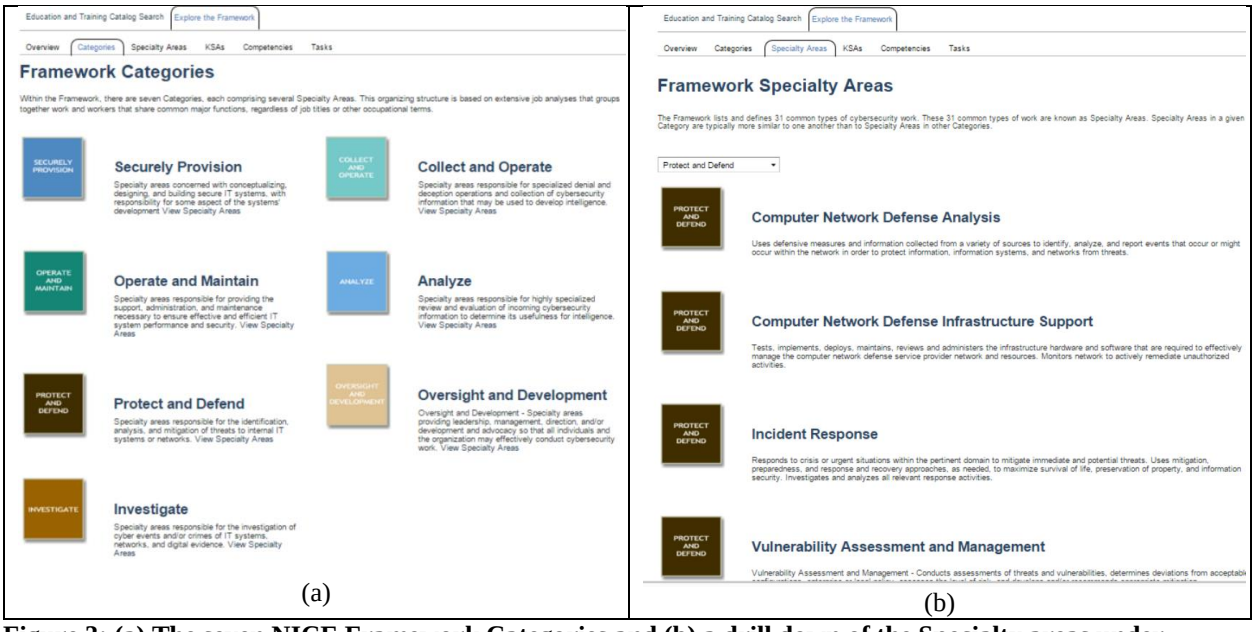

Figure 3: (a) The seven NICE Framework Categories and (b) a drill down of the Specialty areas under Protect and Defend.

John Evans currently works for a large company as part of their IT department. John has been interested in career advancement and has chosen to enter a training and education program for cybersecurity. While researching his options, he explores the interactive NICE Framework to get ideas about what jobs and categories of specialization are available. The interactive framework provides several features to examine specific careers including the knowledge, skills and abilities (KSAs) that represent the "attributes required to perform a job and are generally

demonstrated through qualifying experience, education, or training" (NICCS, 2015). Shown in Figure 3, (a) the seven categories range from Analyze to Operate and Maintain, and Protect and Defend. Looking into the Category of Protect and Defend, John finds a variety of Specialty Areas and short descriptions of each.

After selecting the competency Computer Network Defense, the framework shows a listing of required knowledge, skills and abilities (shown in Figure 4).

Once John has selected this competency as a goal for his training, he would sync his PAL with this list of required KSAs and the TLA would manage, track and monitor his progression along a path of learning activities that will bring him to a the level of proficiency required for success in his future position.

In particular John has set an objective to achieve the initial three KSAs of Computer Network Defense:

1. Knowledge of and experience in Insider Threats
2. Knowledge of common adversary tactics, techniques and procedures
3. Knowledge of Computer Network Defense and vulnerability assessment tools

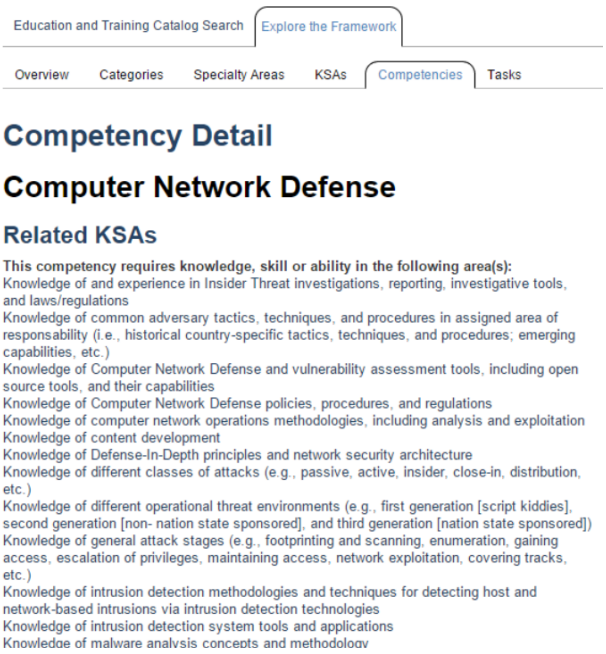

Figure 4: KSAs for Computer Network Defense

Appropriate learning activities can range from classroom lectures to interactive simulations, depending on his availability of time and resources. In the following sections we will discuss activities to train these skills in live, virtual and constructive (LVC) simulation environments that the future TLA may recommend for John.

LVC CYBERSECURITY TRAINING ENVIRONMENTS

1. Knowledge of and experience in Insider Threats in a virtual 3D world

In today's business landscape employees routinely receive training in cybersecurity, but it is often delivered broadly, focusing primarily on overviews of cybersecurity. This is unfortunate because the training fails to address specific components of cybersecurity like those stemming from within the organization or the "insider threat." The insider threat is represented by individuals that have the ability to or at one time had permission to access an organization's data or network structures. Insiders to an organization have multiple advantages, including knowledge of where critical data exists and the ability to access to restricted areas. Insiders can include current and past employees, one-time collaborators, and trusted organizational individuals (Colwill, 2009). Based upon these factors, it is important for organizations to implement training protocols and regimens for specific threats like the insider and to ensure that the training is specific to the company's culture and that employees comprehend the purpose of the training. Furthermore, the method in which the training is conveyed also plays an integral role in organization's ability to protect itself. The usage of novel training practices, such as 3D gaming environments, offers an interactive training method to engage participants in a way that would not be as impactful or lasting if delivered in a conventional classroom setting.

3 Dimensional (3D) Gaming Environment for Training

3D gaming environments provide unique training opportunities that can apply concepts and solutions to increase user understanding; this type of implementation is also called serious games (Cone, Irvine, Thompson, & Nguyen, 2007) . Serious game is an area of gaming that is solely used for training or learning purposes and can be developed to represent a variety of applications. These applications include the ability for users to receive training by assuming different roles or characters in an environment. Serious games provide a unique and beneficial environment that can replicate and logistically control difficult, dangerous, or complicated situations in a practical and safe environment (Schmorrow, Cohn, & Nicholson, 2009). Based upon these aspects, serious games provide a parallel to the dynamic nature of cybersecurity, in particular to an insider-threat training environment. Serious games, like general 3D gaming

environments, can be driven by both proprietary methods and the usage of gaming engines such as Unreal 4 (UE4), by Epic Games, which is rapidly gaining popularity.

Insider Threat 3D Gaming Environment

An insider threat is best illustrated by human behaviors and actions based upon context in a specific area, like an office environment. In order to accurately portray the high-fidelity details needed to depict an insider threat, a gaming environment is required; UE4 is implemented to generate this environment because of UE4's ability, on multiple levels, to provide the imagery, character kinesics, audio, immersive qualities, and interactivity options necessary to offer the best possible representation of what is occurring in an actual insider threat scenario. This type of fidelity is ideal to illustrate the details necessary when proposing training content. Furthermore, UE4 offers the technological ability to depict detail of not only realistic actions of human behaviors, such as walking, in computer-controlled agents, but also provides authentic high-fidelity visuals, portraying assets or terrain features, such as buildings, desks, cubicles, office furnishings, computers, or other items that might be required in the training content. This ability to develop realistic representation creates an immersive environment that aids in the serious game implementation. Also, developers are able to customize content and specific features via programmatic controls of display options, including informational pop-ups or factoids, scenario hints, user progress tracking, and the ability to access what a user has learned.

Development processes

The first step in developing training content in UE4 that depicts a realistic insider threat scenario in an office environment is to develop a roadmap that defines several key variables (Ortiz et al., 2016). These variables include the narrative of the scenario (e.g., the story or what is happening), artistic components (e.g., the type of environment, how it looks, and the level of fidelity needed for the portrayal of events), and the programmatic components (e.g., scenario event actions, pop-ups or factoids, progress tracking, and how the training will be delivered). This variable also includes the application of appropriate views of the scenario (e.g., first-person or third-person). The final variables are the training components, including:

- The goal of the training
- Specifics of the insider threat being portrayed
- Identification of audience
- Plan for assessment of progress, and
- Determination of event conclusion or completion.

Each of these functional areas are equally important and all must be included in order to represent the training components the game is depicting and to aid in determining the effectiveness of the training.

Insider Threat Scenario

The following scenario is an example of an insider threat training application designed through UE4. Figures 5 and 6 depict the scenario's location, an office environment. It is designed to replicate the misuse of computer systems by an employee recruited by their manager, also an insider, to gain unauthorized access to financial information. The manager will be virtual within the scenario and provide tasking for the user. The purpose of this scenario is to raise user awareness of what types of actions comprise an insider threat (e.g., who can be a threat, what type of information they can access, and what means can be utilized to gain access).

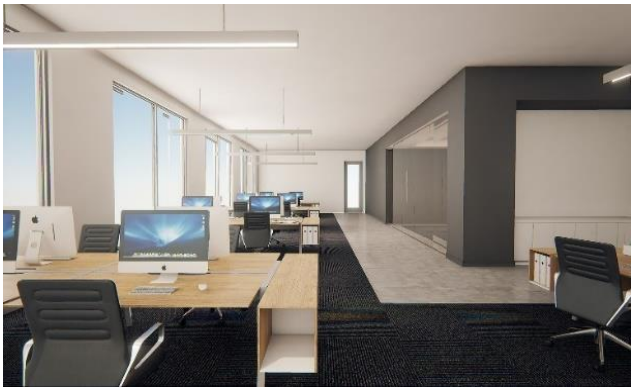

Figure 5: Example UE4 office environment

In the scenario, the user plays the role of an employee within a large financial institution; the scenario contains two narrative levels. In both levels, the user is tasked with trying to access the account of a high-net-worth client. Prior to the beginning of the scenario, the user will receive instructions from the manager regarding tasking. The instructions include the specific assets to be found and how to find them. The user's task is to find information about specific bank accounts (e.g., account number and type). To accomplish these tasks, users will move around the environment finding items of information located in different offices and storage media. In some cases, information will be incomplete, so the user will need to perform additional searches (e.g., folders on desktops), ask other bank staff for information, or make inferences in effort to gather the proper information to access the accounts.

Figure 6: Example UE4 office environment

In the first level of the scenario, the high-net-worth client has placed enhanced protections on some of his financial accounts, thus making account information only accessible at specific times. Additionally, the information is only accessible using access keys that must be found. Moreover, in this level, the user has the ability to access certain features of the account, but does not have full rights to the enhanced features. The goal of this level is to find the account information items requested by gathering access keys (e.g., files containing details of how to acquire hidden passwords, etc.) located within the office environment and during the specific times the account information is available. The user will have the ability to freely roam around the entire office environment to gather access keys; however, if an access key is selected at the wrong time the user will be exposed as an insider and fail. As access keys are acquired, factoids will appear detailing components of insider threats pertaining to where that access key was found (e.g., on a storage media or a password written on a sticky note) and why this can be a cybersecurity theat. This level is designed to be simple in effort to introduce the user to basic aspects of a possible insider threat.

In the second level, which is similar to first but more difficult, the insider is prohibited from accessing any account information related to the high-net-worth client's account. They are told at the outset they are under surveillance for any sign of prohibited activities; however, they have been instructed by the manager to access the accounts regardless. Additionally, the manger has instructed the user to gather the details of the account during the course of the normal work activity to circumvent any suspicions. The user will be provided with the same type of information as in the first level, but they will need to disguise their interest in the account information to not give themselves away as an insider threat. Users can disguise their interest by only selecting access keys relevant to the account information pertinent to where they are in the office environment as instructed by the manager. This means if the manger states for the user to go from the office "A" to the "copier room" then any access keys found along the route are available to gather; however, if a user gathers an access key from anywhere else in the environment they will be exposed and subsequently fail the mission. Toward the end of the level, they will have an opportunity to access the forbidden account information if they have found all the necessary access keys. The goal of this level is to not raise suspicions of IT personnel as to their actions, because it they are caught they will be fired or possibly face criminal charges. Both levels revolve around collecting the same type of access keys with the second being more difficult. The purpose of this scenario is to raise user insider threat awareness by escalating the level of effort that must be executed in effort to accomplish the goal of accessing unauthorized accounts.

2. Knowledge of common adversary tactics, techniques and procedures in a virtual simulation with constructive agent players

Under an AFRL SBIR, our team is developing the Cyber Security Instruction Environment (CYSTINE). CYSTINE is a training system that uses the Soar Technology Dynamic Tailoring System (DTS) framework to create dynamic training scenarios that respond to the skill of the trainee. It employs cyber defender cognitive agents, modeled using the Soar cognitive architecture. The system follows an Event-Based Approach to Training (EBAT) as described in Johnston, Cannon-Bowers and Smith-Jentsch (1995). Our updated EBAT implementation combines the advantages of scripted and discovery-oriented simulation-based training, while addressing the limitations of each. This is achieved within the DTS by linking learning objectives and performance assessment to key situational events that can be

realized by adapting the conditions or "state" of the network environment. Since there are multiple acceptable paths for accomplishing each key event, a constrained set of expected response actions and attributes (Woods, Stensrud, Wray, Haley, & Jones, 2015), and the time window within which those actions should occur, are defined. CYSTINE's environment allows free play and the DTS employs adaptive tactics to create situations/events within the environment that support the selected learning objectives, enabling students to practice skills without requiring the instructor to author individual scenarios. It uses Soar agents to provide dynamic, cognitively realistic adversaries – defenders that offer active opposition to the student. At the same time, it monitors and assesses student proficiency in order to provide scaffolding and feedback, maximizing each student's learning experience. The result is a simulation-based training system that adapts and learns with the students without placing an unreasonable burden on instructors (Schmorrow, et al., 2009).

To define the components of the CYSTINE training system, we refer to the conceptual model of learning shown in Figure 7, adapted from Oser, Cannon-Bowers, Salas, & Dwyer (1999). The four main functions in Oser's model, shown in blue, center around the goals of the Training Audience, consisting of the student(s) and any additional training team members and/or role players needed. The students' goals define the Task/Training Objectives that feed the selection of learning strategies and tools, which then establish the parameters of the training environment to be experienced by the students and role players.

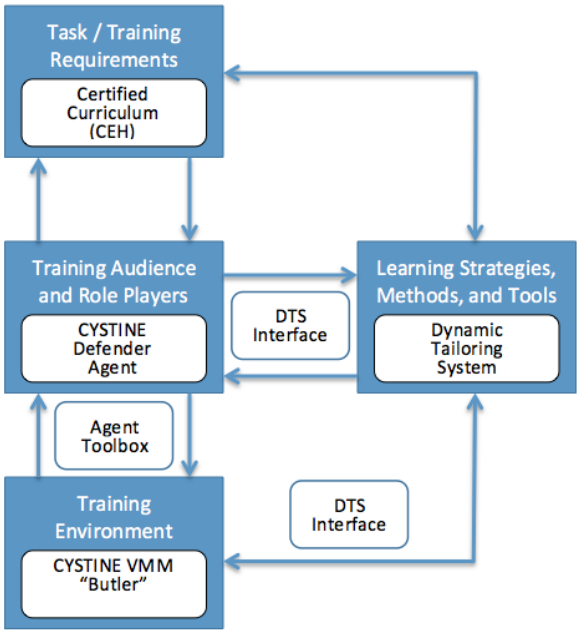

Figure 7: High-level Model of CYSTINE Training System

The two main innovative software components are 1) *cognitively realistic defender agents* to supplement or replace role players, which can also be complemented with additional attacker agents leveraging work from our ONR sponsored development of a Simulated Cognitive Cyber Red-team Attacker Model (SC2RAM) (Jones et al., 2015), and 2) adaptive training and instructional methods, realized by expansion of our *Dynamic Tailoring System* to include performance measurement and instructionally relevant adaptation of the training experience.

Cognitively Realistic Defender Agents

One of the elements missing from many cyber operations and penetration testing training environments is an element of active opposition. The instructor assigns students a task or objective, and the student then practices within a virtual environment. These environments can have static defenses (firewalls, antivirus, etc.), but typically lack any active defenders that might monitor logs, block connections, and so on. This is akin to training fighter pilots against adversaries that do not fight back. This is unfortunate for two reasons: first, it trains cyber operators to behave as though adversaries don't exist, and second, they are missing an opportunity to tailor the student's learning experience through adjustable defender behavior.

For CYSTINE, we are employing a cognitively realistic (behavior based on human cognition) defender agent in order to provide active defense within the training environment. We are designing and implementing the agent in the Soar cognitive architecture, based on interviews with SMEs from Merit and Eastern Michigan University (EMU).

Adaptive Training and Instruction

Following instructional methodologies prevalent in other Air Force simulation based training such as the Distributed Mission Operations (DMO), CYSTINE's goal is to allow USAF cyber operators to "train as they fight" (Andrews & Bell, 2009) with adaptive adversaries and appropriate consequences to actions taken. As in real operations, not all operators are at the same skill level and require different levels of feedback, coaching and scenario complexity to be able to effectively execute the mission. To manage the instructional process, CYSTINE uses SoarTech's DTS, which

maintains a model of student proficiency and adapts the difficulty of the training to the individual trainee while providing detailed feedback to the instructor for evaluation and coaching.

The DTS measures training performance in two ways. The first involves capturing objective data of the actions and activities within the environment, including student and agent actions synchronized with network activity. The second, as in the DMO, involves providing a means for instructors and observers to capture their subjective measures in real time while the exercise is underway. This has been shown to be an effective tool for organizing debriefs and feedback sessions around key performance events (both successes and failures). These measurements are available to the instructor and feed into the DTS student model to inform of macro-adaptation of training, i.e., selection of remediation and the focus of the next training event, and can be used in real-time to drive micro-adaptation of the on-going training exercise such as changing the difficulty level or type of challenge introduced (Snow, 1977).

3. Knowledge of Computer Network Defense and vulnerability assessment tools in a live simulation exercise

Although theoretically understanding the necessity of cyber security provides insight on cyber challenges, applied training regularly ensures readiness against adversaries and depicts the full illustration of the security posture of a system. Red team – blue team exercises implement such applied training methods; these applications were first used by the government for military war gaming practice. As security became a growing concern for the world market, this type of training expanded into use for information security systems. The goal of the cybersecurity training application is to not only pinpoint holes in security, but also to train security personnel and management, much like the original motive.

Currently, several companies and government entities use red team – blue team exercises to practice aspects of security and to attempt to remain on the cutting edge. For instance, since 2000, the five United States service academies have participated in an inter-academy Cyber Defense Exercise (CDE) exercise. This friendly competition provides an opportunity for students across the various academies to test their knowledge of cyber defense by attempting to "implement an attack or exploit, defend against such attack… [and] implement defensive measures in securing the network against external attacks" (Schepens, Ragsdale , Surdu, & Schafer , 2010)

The Cyber Defense Exercise simulations consist of two opposing sides. The red team represents the adversary, who will attempt to identify and exploit vulnerabilities, and the blue team represents the defensive side that will attempt to keep the red team from penetrating their system. Red team members would be able to understand how attacks are implemented. This gives a perspective that otherwise would not be possible without hands-on training; being able to comprehensively understand the thought pattern of an adversary will aid in the development of defensive measurement against the attack. Furthermore, implementing such attacks allows trainees on the blue team to know how to combat the attack and understand first-hand how such an attack can affect their system. In the CDE, a group of cadets from a certain academy would represent the red team while an opposing academy would make up the blue team. Outside of the realm of cadet competition and training, this type of simulation-based training is used in the workforce to aid in the development of the cyber-workforce. In those type of scenarios, the opposing teams would be made up of coworkers. These exercises have proven to be beneficial to the cadets by providing awareness of how to think like an adversary, manage security challenges, and remain on the forefront of a rapidly expanding field of computer science. Moreover, this method has provided a cost-effective way to evaluate security and identify key changes that should be made to a system.

However, red team – blue team exercises generally take place as an applied training measure for participants that are well aware of the toolbox of an adversary. This toolbox is substantial, and without prior in-depth training may be overwhelming to novices. When red team – blue team training emerged in the cyber world, it was done as friendly competition among the military academies by cadets that have been trained on several aspects of the adversary's toolbox. The simulation allowed the cadets a chance to apply learned methods and comprehend first-hand how attacks can impact the system; it also provided the cadets on the blue team a challenge to defend against these attacks.

The cyber security community overall may not have the opportunity to be exposed to training methods like those practiced at the military academies. Therefore, there is a necessity to bridge the gap and develop resources for professionals and emerging professionals to accommodate and provide the same type of enhanced learning experiences in simulated virtual worlds such as those previously discussed.

ROAD AHEAD

These three enhanced learner experiences for cybersecurity demonstrate examples of innovative and diverse training that could be used to support the development of NICE framework KSAs needed for the growing cybersecurity workforce. Our research on developing an infrastructure for the ADL PAL and the TLA architecture under FLUENT will begin to demonstrate the ability to integrate simulation and scenario based LVC training experiences within the PAL vision to address the demand for flexible, tailored learning in this challenging domain of expertise.

ACKNOWLEDGEMENT

This material is based upon work supported by the Advanced Distributed Learning (ADL) Initiative under Contract No. W911QY-16-C-0019. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Advanced Distributed Learning (ADL) Initiative.

REFERENCES

Andrews, D., & Bell, H. (2009). A Virtual Environment Application; Distributed Missions Operations. In J. Cohn, D. Nicholson, & D. Schmorrow (Eds.), *The PSI Handbook of Virtual Environments for Training and Education* (Vol. 3, pp. 77-85). Westport, Connecticut: Praeger Security International.

Colwill, C. (2009). Human factors in information security: The insider threat - Who can you trust these days? *Information Security Technical Report*, 186-196.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security, 26*(1), 63-72.

CSO. (2015, July 28). *Cybersecurity Job Market to Suffer Severe Workforce Shortage*. Retrieved from CSO Online: http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

Department of the Air Force. (2014). *AFSC 17X Cyberspace Operations Officer.* Washington, DC. Retrieved from http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/cfetp17x/cfetp17x.pdf

Johnston, J. H., Cannon-Bowers, J. A., & Smith-Jentsch, K. A. (1995). Event-based performance measurement system for shipboard command teams. *Proceedings of the 1st International Symposium on Command and Control Research and Technology*, (pp. 274-276). Washington, DC.

Jones, R. M., O'Grady, R., Nicholson, D., Hoffman, R., Bunch, L., Bradshaw, J., & Bolton, A. (2015) "Modeling and Integrating Cognitive Agents Within the Emerging Cyber Domain." *Proc. Interservice/Industry Training, Simulation, and Education Conference*.

National Initiative for Cybersecurity Careers and Studies. (2015). *National Initiative for Cybersecurity Careers and Studies*. Retrieved from About the NICCS Training Catalog: https://niccs.us-cert.gov/training/tc/search

Oser, R. L., Cannon-Bowers, J. A., Salas, E., & Dwyer, D. J. (1999). Enhancing human performance in technology-rich environments: guidelines for scenario-based training. In E. Salas (Ed.), *Human/Technology Interaction in Complex Systems* (Vol. 9, pp. 175-202). Stanford: JAI Press.

Regan, D. (2013). *Advance Distributed Learning: Enabling Enhanced Learning Experiences* . Retrieved from Advance Distributed Learning: http://www.adlnet.org/wp-content/uploads/2013/04/regan_adl_enhanced_experiences_else_2013.pdf

Schepens, W. J., Ragsdale , D. J., Surdu, J. R., & Schafer , J. (2010). *The Cyber Defense Exercise: An Evaluation of the Effectiveness of Information Assurance Education.* Retrieved from University of Maine, Fort Kent: http://perleybrook.umfk.maine.edu/slides/fall2010/ELC200/bh-fed-03-dodge.pdf

Schmorrow, D., Cohn, J., & Nicholson, D. (2009). T*he PSI handbook of virtual environments for training & education: Developments for the military and beyond* (Vol. 1). Westport, CT: Praeger Security.

Schmorrow, D., Nicholson, D., Lackey, S. J., Allen, R. C., Normal, K., & Cohn, J. (2009). Virtual Reality in the Training Environment. In D. A. Vincenzi, J. A. Wise, M. Mouloua, & P. A. Hancock (Eds.), *11 Human Factors in Simulation and Trianing* (pp. 201-228). Boca Raton, FL: CRC Press.

Snow, R. E. (1977). Individual differences and instructional design. *Journal of Instructional Development*, *1*(I), 23-26.

Woods, A., Stensrud, B., Wray, R., Haley, J., & Jones, R. (n.d.). A Constraint-Based Expert Modeling Approach for Ill-Defined Tutoring Domains. *Proceedings of the Florida Artificial Intelligence Research Society (FLAIRS-28).* St. Pete Beach: AAAI Press.