Integrating Cyber Protection Teams into Training Exercises

By Col. Jon Erickson

Army National Guard Cyber Protection Team participating in Northern Strike. (Photo by Staff Sgt. Katherine Jacobus)

The 86th Training Division plans, delivers, and enables realistic and relevant training in complex and austere training environments to prepare commanders, Soldiers, and units for multi-domain large scale combat operations (LSCO). This type of training is only available to most Army Reserve units at the Combat Support Training Exercise (CSTX) in Fort McCoy. In recent years, CSTX has been the center of innovation, where over 7,000 Soldiers have been exposed to new capabilities and delivered feedback to the capability providers. New to the CSTX, was the participation of the Army Reserve Cyber Protection Brigade (ARCPB).

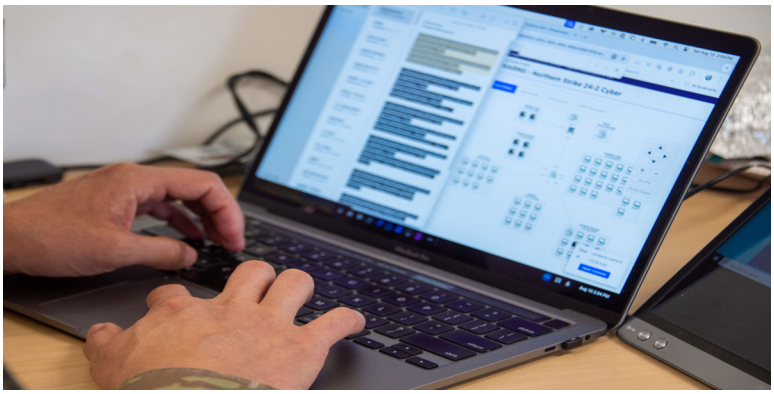
Incorporating a CPT into a Training Exercise:

As part of the exercise scenario, the CSTX division commander's G6 submitted a request for forces (RFF) for a Cyber Protection Team (CPT) to mitigate a cyber-attack that the division was experiencing. The ARCPB assigned CPT 183 to serve under the operational control of the CSTX division commander. CPT 183 received an order from the G6 to determine what vulnerabilities were exploited and recommend how the G6 can prevent future attacks from succeeding. CPT 183 employed their virtual Deployable Defensive Cyberspace-Modular kits in the Persistent Cyber Training Environment (PCTE) cyber range to conduct initial network reconnaissance, identify cyber key terrain, uncover what vulnerabilities were exploited, and determine the enemy's most likely and most dangerous courses of action. Their final task was to brief the Division G6 on best practices and the actions required to prevent future cyber intrusions.

CPT 183 is assigned to the Southwest Cyber Protection Center (SWCPC) at Fort Gillem, GA and participated in CSTX during their Battle Assembly training from Aug. 3-4. The 86th Training Division's Cyber Observer, Coach/Trainer (OC/T) team initiated the cyber exercise and managed the event through PCTE. As CPT 183 accomplished specific cyber tasks in PCTE, these activities were captured and simulated in the Cyber Battlefield Operating System Simulation (CyberBOSS) platform. This training exercise demonstrated three concepts that should be value added for the Army moving forward. The first concept was demonstrating that cyber training events can be executed remotely and linked to Army Reserve Collective Training Exercises. The second concept proved that OC/Ts are capable of remotely observing and evaluating a CPT's performance during their missions. The third and final concept was demonstrating how CPTs across the force can receive technical training value when partnering with other units during training events.

Due to CPT 183's participation, the 86th conducted a first-of-its-kind proof of concept that overcame several technical hurdles and captured live cyber activities on a cyber simulation platform. Maj. Eric Fong, the 86th's cybersecurity engineer, partnered with Program Executive Office – Simulation, Training, and Instrumentation

(PEO-STRI) and U.S. Army Combat Capabilities Development Command (DEVCOM) to receive activities from PCTE and accurately capture and replicate CPT activities in near real-time in CyberBOSS. The main goal of inserting a CPT into a CSTX was to demonstrate that a blended cyber-kinetic training exercise more realistically depicts the modern warfare scenario. Current practice for training exercises will simulate defensive cyber actions by creating an inject in the Master Scenario Event List (MSEL) and handing it to the training audience as a “white card”. The “white card” simply states what the cyber-attack is conducting on the network without any effects. Participating CPTs can conduct near real-time defensive operations which will impact the training audience and drive what MSEL injects to execute.



Army National Guard Cyber Protection Team conducts a cyber attack on a simulated powerplant. (Photo by Staff Sgt. Ariel Solomon)

According to the SWCPC commander, Lt. Col. Eric Booker, “Cyber Protection Team 183’s participation in the exercise allowed me as a commander to observe the team operate on collective tasks. Moreover, I was able to watch junior officers and NCOs lead in a small group setting. The back brief session alone was invaluable training for the Soldiers as it gave them practice in briefing the network owners on mission findings. Great training conducted by Soldiers from their home station!” CPT 183’s participation allowed developers for PEO-STRI and DEVCOM to observe how a CPT operated on a mission, receive feedback on how the exercise went, and determine the direction for future enhancements.

Way Ahead:

Building upon the success of this proof of concept, the next step is for the Cyber OC/T team to collaborate with G6 and DEVCOM to create scenarios within CyberBOSS that can directly affect the exercise network. Adding this capability to the current proof of concept would create a fully integrated, end-to-end Live, Virtual and Constructing (LVC) system into the exercise. CyberBOSS would function as the conduit linking the virtual effects in PCTE to the live effects on the exercise network. Where a certain cyber effect may create too much risk to either the network or to training units, CyberBOSS can be used to execute the effect in its sandbox environment to create constructive effects that drive what MSEL injects to implement.

One final initiative for creating a fully integrated LVC system is to allow other training exercises and training divisions to receive the benefit of a CPT’s participation. As the Division G6 is tasking the CPT to conduct various missions in PCTE, CyberBOSS would capture all CPT activities and emulate those activities in the cyber simulation platform. In future training exercises where a CPT may not be available, the training division could employ a virtual CPT that is emulated by CyberBOSS. This type of capability would allow any training exercise the benefit of incorporating a constructive CPT into its scenario and to choose what CPT missions to execute in the exercise.

Bio

COL Jon Erickson, is a Cyber and Signal officer and a Functional Area 26B (Information Systems Engineer) in the U.S. Army Reserves serving as the Cyber Director for the 335th Signal Command (Theater). He is a graduate of the Army War College. His previous assignments include serving as a Brigade S3 and a Battalion Commander in the 335th Signal Command, and Cyber Effects Chief for the 86th Training Division. Lt. Col. Erickson has three combat deployments – Iraq, Afghanistan, and Kuwait – and one overseas tour in Germany.