

Employing High Performance Computing to Realize a Cyber Quick-Reaction Training Environment

Brian R. Castello, Douglas W. Hire & John J. Tran
261st Network Warfare Squadron
Van Nuys, California
{brian.castello, douglas.hire, john.tran}@ang.af.mil

Robert F. Lucas & Ke-Thia Yao
Information Sciences Inst., USC
Marina del Rey, California
{rflucas, kyao}@isi.edu

Dan M. Davis
HPC-Education
Long Beach, California
ddavis@hpc-educ.org

ABSTRACT

While it is a supportable assertion that the conceptualization and realization of Forces Modeling and Simulation (FMS) strategies are well understood for kinetic warfare, the same assumption does not yet hold true for non-kinetic warfare, *e.g.* cyber warfare. The development of a strategy with respect to FMS cyber warfare is still evolving. To date, successful annual cyber exercises, such as Cyber Flag and Cyber Guard, offer promising introductions into the development of FMS tactics and strategy. The fact remains that these large-scale exercises cost millions of dollars to implement and support. However, with the expansion of open source tools and the enhancement of hardware services, such as High Performance Computing (HPC) configurations, a cost-effective and adaptive solution is not only desirable but also tenable. In response to this, we propose a Cyber Quick-Reaction Training Environment (CQRTE). The CQRTE concept is based on the philosophical tenets of McRaven's highly regarded *The Theory of Special Operations*, which was an examination of eight important treatises on small warfare operation and strategy.

This paper focuses on our Research and Development (R&D) efforts, which used HPC to stand up a low-cost fully operable cyberspace training and exercise environment. To the best of our knowledge, it is the first of its kind. The project has demonstrated how CQRTE can effectively model warfare principles within the context of cyberspace operations and, when combined, these principles can achieve relative superiority. The success of the envisioned CQRTE can serve as a guiding beacon for those combatant organizations whose mission-set requires continuous training and modeling, as well as the development of tools and tactics in the cyberspace domain.

ABOUT THE AUTHORS

John J. Tran is a Major in the California Air National Guard. He received both his BS and MS Degrees in Computer Science and Engineering from the University of Notre Dame, where he focused on object-oriented software engineering, large-scale software system design and implementation, and high performance parallel and scientific computing. He has worked at the Information Sciences Institute (ISI), University of Southern California (USC), the Stanford Linear Accelerator Center, Safetopia, and Intel Corporation. His current research centers on Linux cluster engineering, effective control of parallel programs, and communications fabrics for large-scale computation. His tours of duty included the White House Communications Agency and Kirkuk Regional Air Base (Iraq), where he was the Communications Squadron Commander.

Brian R. Castello is a Lieutenant in the California Air National Guard and has served active duty tours with the 5th Combat Communication Group. On active duty, he served in Iraq and in many locations around the United States. As a civilian, he is a Systems Engineer at Space Systems/Loral. He received both his BS in Electrical Engineering and MS in Aerospace Engineering from the California Polytechnic State University, San Luis Obispo.

Douglas W. Hire is the Commander of a Cyber Operations Squadron in the California Air National Guard. Lieutenant Colonel Hire has also served as a Combat Communications Squadron Commander deploying in this capacity to overseas locations. He received his BS from Southern Illinois University and his MS in Telecommunications Management from National University. Colonel Hire has completed strategic studies at the Air War College, Maxwell AFB, as well as the Joint Forces Staff College, Norfolk VA.

Robert F. Lucas is a Deputy Director of the Information Sciences Institute at the University of Southern California and leads the Computational Sciences Division. He is a Research Associate Professor in the USC Department of

Computer Science. At ISI he manages research in computer architectures, VLSI, compilers, and other software tools. He was the principal investigator on the JESPP project from 2002 to 2011, which first implemented GPU acceleration in high performance computing for battlefield simulations. Prior to joining ISI, he served as the Director of High Performance Computing Research for NERSC at LBNL, the Deputy Director of DARPA's ITO, and a researcher at the Institute for Defense Analyses, supporting the National Security Agency. Dr. Lucas earned BS, MS, and PhD degrees in Electrical Engineering from Stanford University.

Ke-Thia Yao is a research scientist in the Computational Systems and Technology Division of the Information Sciences Institute at USC. His primary research interest is helping people understand large complex systems and data sets. He has conducted data management research on the JESPP project with the goal of supporting very large-scale distributed military simulation involving millions of entities. Within the JESPP project he developed a suite of monitoring/logging/analysis tools to help users better understand the computational and behavioral properties of large-scale simulations. He received his B.S. degree in EECS from UC Berkeley, and his M.S. and Ph.D. degrees in Computer Science from Rutgers University.

Dan M. Davis was the JESPP project director for the Information Sciences Institute at USC, where he now consults on distributed DoD simulations. Earlier, as Assistant Director of the Center for Advanced Computing Research at Caltech, he managed Synthetic Forces Express, bringing High Performance Computing to DoD battlefield simulations. Other positions include having been a Director at the Maui High Performance Computing Center and a Software Engineer at the Jet Propulsion Laboratory and at Martin Marietta. He saw duty in Vietnam as a USMC Cryptologist and retired as a Commander, U.S.N.R. He holds B.A. and J.D. degrees from the University of Colorado.

Employing High Performance Computing to Realize a Cyber Quick-Reaction Training Environment

Brian R. Castello, Douglas W. Hire & John J. Tran
261 Network Warfare Squadron
Van Nuys, California
{brian.castello, douglas.hire, john.tran}@ang.af.mil

Robert F. Lucas & Ke-Thia Yao
Information Sciences Inst., USC
Marina del Rey, California
{rflucas, kyao}@isi.edu

Dan M. Davis
HPC-Education
Long Beach, California
ddavis@hpc-educ.org

INTRODUCTION

One need look no farther than today's headlines to recognize that the United States is under constant attack by very large, globally dispersed, and technically competent cyber adversaries (Lynn 2010). In order to defeat this more numerous and very determined enemy, the Nation must find an effective way to offset the superiority of their numbers and the relentlessness of their attacks. Faced with a similar challenge in the more kinetic world, students of history have advanced an approach which relies on using precision and focus in order to offset numbers and zealotry (McRaven, 1993). One advantage that is possessed by the U.S. is that of advanced technologies that support excellent training. That training has been tested and found decisive on the battlefield (Horowitz, *et al.* 1995).

As noted above, there have been significantly high levels of implementation of Forces Modeling and Simulation (FMS) for kinetic warfare and subsequent analyses of the associated strategies. The same cannot be said for the field of cyber warfare. The development of an FMS strategy for cyber warfare is still evolving. Some of that evolution is evidenced by successful annual cyber exercises, such as Cyber Flag and Cyber Guard, which have attracted national attention (Cyber Flag, 2013; Cyber Guard, 2014). These offer promising foundations for the development of cyber-FMS tactics and strategy. One of the major impediments to more fully utilizing these methods is the fact that these large-scale exercises cost millions of dollars to implement and support. With the expansion of open-source tools and the ready accessibility of High Performance Computing (HPC) capabilities, a cost-effective and adaptive solution is not only desirable, it is essential.

BACKGROUND

Forces Modeling and Simulation has already been shown to provide a significant augmentation to training, analysis, and evaluation for the Warfighters. That impact has been seen on the battlefield (U.S. Government, 1995) and in experimentation for analysis and evaluation (Lucas & Davis, 2003). High Performance Computing has shown the ability to enable these simulations to scale up the ten million semi-automated forces entities (Gottschalk, *et al.*, 2010). Using HPC instead of tens of thousands of live participants has a number of benefits ranging from cost savings all the way to the ease of automated logging of entity activities, location, and status.

The cost of running full-scale exercises is very high, *e.g.* Millennium Challenge 2002 (MC02) is reported to have cost \$250 million dollars (van Riper, 2004). While smaller, Cyber Flag and Cyber Guard are also reputed to have been very costly. Large exercises also require extensive Internet Connection Sharing (ICS) models, cumbersome logistics and entail schedule disruptions and travel costs that do not necessarily translate into increases in the ultimate value of the exercises.

Small unit exercises have proven to be very effective in the kinetic world. One of the most well-known was the adoption of "America's Army" as a training tool. Originally conceived and implemented by Professor Michael Zyda, then at the Naval Postgraduate School in Monterey California, it was intended to be a first-person-shooter game to be used by the Army as a recruiting tool. However, it was discovered that active duty soldiers were also playing it on-line and that their performance and skill levels improved (Jean, 2006). Now an entire community has sprung up to support the America's Army systems.

Similarly, in the cyber warfare area, there is a need for small unit FMS. Some say that wars are fought, not by mighty armies, but by small units. We assert that this truth is a basis for the need for small unit simulations that will enable them to perfect their skills, ascertain their weaknesses, and correct their faults.

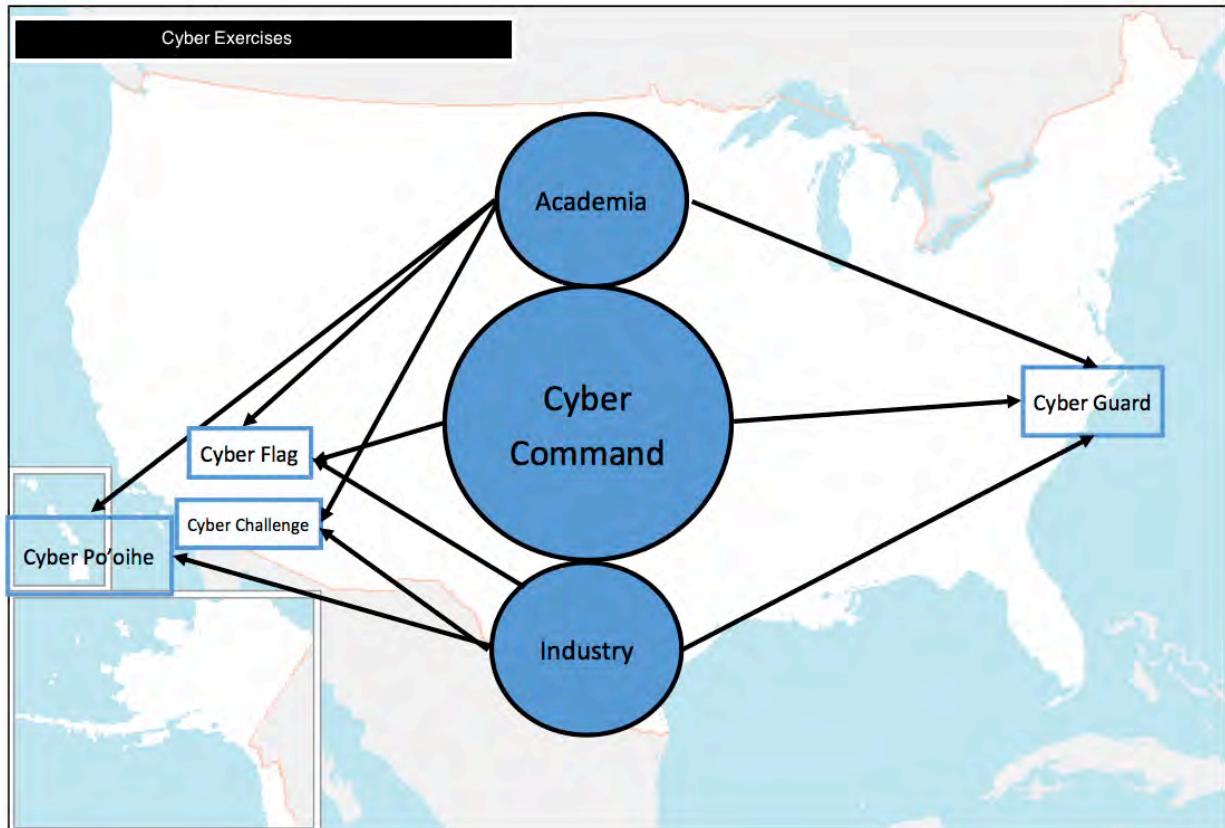


Figure 1: Cyber Exercises

The proposition of the inevitability of an all-out Cyber Armageddon is debatable at best (Libicki, 2009). However, what is clear is that, as the cyber war-fighting paradigm becomes a major focus of key decision makers, the demand for training, force development, and strategic planning approaches increasingly come into play (Tran, 2014). To address these needs, a number of cyber exercises have been held annually. Figure 1 is illustrative of the roles of various institutional players in these exercises. We observe a common element in all of these exercises: collaborative efforts from industry, the military, and academia are essential for their success. Contributions from the aforementioned triad synthesize into the spirit cooperation between the academic community (research), the military community (consumers of R&D), and industry (strategic partners).

The CQRTE System

The 261st NWS has collaborated with the University of Southern California's Information Sciences Institute (USC/ISI) and a National Laboratory in the development of a Cyber Quick-Reaction Training Environment or CQRTE (pronounced *kwerty*). CQRTE was specifically designed as a multi-discipline and multi-organization system to support small-scale non-kinetic exercises by effectively modeling warfare principles and doctrines within the context of cyberspace and cyber warfare operations.

CQRTE's capabilities are as follows:

- Leverages low-cost commodity hardware
- Leverages no-cost open-source software
- Automates exercise setup and teardown
- Provides scalable exercise configuration
- Facilitates a system that is automation driven
- Supports diverse training objectives
- Assures logging and analytics for complex data
- Enables integration with ICS systems

The success and wide-spread adoption of the envisioned CQRTE can serve as a functioning example for those combatant organizations whose mission-set calls for continuous training, as well as making effective use of modeling and simulation to develop the tools and tactics in the cyberspace domain. It is a replica model with which squadron and battalion-level organization can design, organize, and host cyber exercises with minimal cost.

CQRTE's Role in the National Cyber Defense Spectrum

Many of the larger events such as Cyber Guard and Cyber Flag are effective at bringing many organizations together from across the nation, but are not plausibly appropriate for individual units or smaller scale training exercises. This is due to the size of the infrastructure and the magnitude of the needed workforce to maintain and operate these large exercises. CQRTE is carefully designed for individual units that need to provide training and certify qualifications for their members, all the while maintaining a record of low cost accomplishment. Cyber training and emulation is not a once- or twice-a-year operation and will require periodic updates to the hardware and services required, but these upgrades are not anticipated to be cost prohibitive. CQRTE is designed to be small and implemented in a way that allows it to be adjustable to support many training missions and exercises.

CYBER CHALLENGE 2015

Cyber Challenge was designed as a proof of concept evolution for the cyber warfare community. Originally, it was intended to be performed over four Uniform Training Assembly (UTA) weekends, which are made up of two days of two UTA's each, totaling sixteen hours of training, but often running longer. This first exercise was run on a single three-day weekend.

The Cyber Challenge exercise was envisioned as an annual event that would bring cyber professionals together in a realistic training environment. Cyber Challenge 2015 tested the skills of the players and demonstrated the latest in cyber protection tactics to the observers. Future exercises will do so as well. The plan to start with an introductory brief of leaders from industry and the Department of Defense was intended to establish a collaborative and engagement environment. This segment of the exercise usually will involve a table-top exercise and an explanation of CQRTE and its capabilities. The following days consisted of demonstrations of cyber protection tactics and operational capabilities by highly qualified Computer Network Defense (CND) elements and Cyber Protection Teams (CPTs) made up of Army and Air National Guard members.

There were two tracks presented at the exercise:

- A senior officer track to consider policy and management issues for the topics at hand
- A technical track with operators actually performing validated procedures

During the "senior discussion" track, we table-topped a hypothetical scenario based on the script described below. The focus of the discussion was: given a disaster scenario where a cyber asset is under attack, "What are the trigger points and what is the path of activation of a uniformed military member?". Figure 2 describes a notional sequence of events leading to bringing the California CPTs and CNDs on-site. We note the set of ideas presented here is an outcome from the discussion; it is not a definitive doctrine. In fact, one could argue that, given the lack of a clearly defined doctrine, the presented information is a good starting point for policy development and is germane to the issues at hand.

The "technical" track is the execution of the direction from the post-planning "conference" described above. In other words, we assume that a successful sequence of trigger events has taken place and therefore the California CND and CPT teams have been activated and have been brought on-site. CQRTE formulated a flat Command and Control (C2) structure that included an incident commander (aka the "pit boss") who interfaces with the battle captain and "higher ups." The incident commander, in theory, must respond to the State hierarchy all the way up to the Governor. There is a notional switch-over point to federal responsibility, once a threat actor is identified as a nation-state actor. The dual-hatted responsibilities of an incident commander are well documented in literature (Scavo, Kearney & Kilroy, 2008). Historically, the act of responding to this problem, if not pre-planned, can lead to disastrous C2 arrangements. As an example of this we would call to attention our nation's response to Hurricane Katrina (Schneider, 2005).

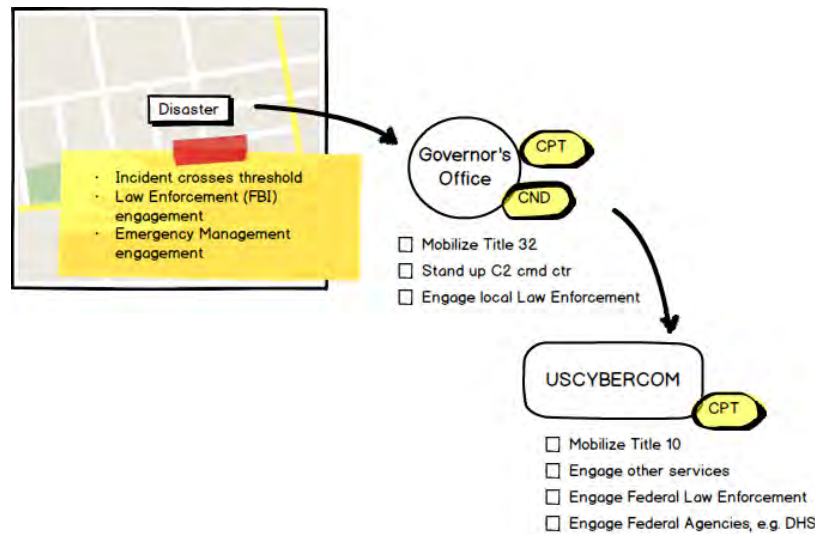


Figure 2: Notional flow of events. This serves as the initial discussion point for the tabletop exercise.

The Story (Scenario)

The original exercise plan began with the blue team CPT waiting for a plane to land at Los Angeles International Airport (LAX), at which time terrorists took over the air traffic control system computer network. The team's envisioned goal was to stop the terrorists before that plane and several other incoming flights, all of which are circling the airport, ran out of fuel and crashed. The planned scenario would include:

- Airport network and ATC systems were fully compromised.
- The tower was to lose its ability to communicate with planes in the air and on the ground.
- Runway lights (ICS) were to be extinguished.
- Critical efforts were to focus on the ability to communicate across the network, stem the attack, and return the ICS systems to operational.

Rules of Engagement

During Cyber Challenge, the participants were instructed to abide by following rules. These rules allowed us to maintain an operational network infrastructure and provided a successful adversarial environment to test real-life issues.

- Participants were instructed to operate in accordance with the CPT constructs.
- Blue Team participants were not allowed to access or modify any other Blue Team's information.
- Blue Team participants were not allowed to attack back.
- Blue Team participants were not allowed to modify the network.

Since our Red Team was fairly new, we did not impose too many restrictions on them in this first exercise. This intent is to strike a balance between meeting the learning objectives and providing a non-trivial exercise experience.

Injects

Blue Teams were instructed by the exercise controllers to respond to scenario events or perform additional tasks. All exercise directions or changes in status, called scenario injects, were hand-delivered by the controllers. When teams had completed an inject, they were directed to notify the team judge and document their activity through completion of reports in the Blue Team's Master Station Log.

The purpose of the injects was to evaluate the C2 and technical skills of the Blue Team participants, especially under conditions of duress. The injects were not designed to “trick” or create unattainable conditions. Table 1 summarizes injects that were used during the exercise. In fact, upon closer examination, one can conclude injects #2 and #4 were designed as hints aimed at helping the Blue Teams to navigate the fog of war.

Table 1 - Injects

#	Description	Time	Blue Action	Red Action
1	Setup Website	0930	Update status of Airport recovery on the internal web site. IP address: Blue 1:172.21.0.22, Blue 2:172.22.0.22	None
2	Security Patch	1000	Install Security Patch on all windows computers	Provide “Security Patch” to judges for delivery to Blue Teams.
3	Key personnel removal	1240	Select desired personnel to be removed	None
4	Announcement of rogue wireless device on the network	1400	Track down the culprit by identify the IP address, MAC address, make, model and firmware of the wireless device	Prevent Blue from obtaining the desired information

Critical Services

In addition to defending the network, another important aspect of the CND’s and CPT’s mission is to maintain services. This requirement is in line with Mission Assurance. The ability to maintain the “status quo” on a network is an expected requirement for Blue Team. The following services were designed to be operational throughout the entire exercise.

- Runway Lights
- Control Tower Radars
- Administrative Network Services
 - DNS, DHCP
 - Email Server
 - File Server
 - Web Server

Currently CQRTE does not have an automatic way to measure the availability of the network services. Instead, we rely on judge’s manual score-keeping. In an ideal setting, CQRTE would provide an automated tool to measure the effectiveness of the Blue Team’s ability to maintain services.

Red Team Actions

Before the Cyber Challenge Exercise, Red Team members had already been implanted into the Blue Enclave and had established a foothold. During the exercise, the Red Team members were to attempt to maintain persistence, escalate their computer access privileges, disrupt critical services, and ultimately disable the runway and air traffic control towers. The Red Team had built a number of exploits and attack vectors. These included weaponized Adobe Acrobat (.pdf) files, Trojan backdoors, and denial of service self-replicating worms. These tactics follow closely the Tactics, Techniques and Procedures (TTPs) described in *Red Team Field Manual* (Clark 2014).

MSEL

The Master Scenario Events List (MSEL, pronounce “measle”) is the overall guidance for the exercise activities. The following tables are representative of the schedule during the exercise. There were four administrative injects, three reporting periods and four main periods of activity on Saturday.

EXERCISE FLOW

In order to map CQRTE to a real-world cyber mission, we focus here on the four stages of cyber activities. They are: (1) map the network, (2) harden the network, (3) hunt the adversary, and (4) maintain and restore services. We added a “Chaos” period. In practical terms, this period is used to measure the effectiveness of the Blue Team’s ability to operate in a stressful environment. The use of this method is not uncommon and could be compared to those found in Operation Readiness Inspection (ORI) exercises. As with any military exercise, a battle rhythm defines the operational cadence. Cyber Challenge is no different (Table 2). It is important to note that this information was not made available to Blue Team participants until after the exercise; this decision was made to maintain the fog-of-war realism.

Table 2 - Battle Rhythm

Time	Event	Blue Action	Red Action	White Action	Desired Outcome
Period 1	Set up Inject #1	Hardening	Enumerating	Evaluate performance Deliver injects	B: Harden systems R: Map of Network
	<i>Reporting</i>	<i>Provide status on Hardening efforts</i>	<i>Map of the network</i>	<i>Grade B & R</i>	
Period 2	Restore Services Inject #2	Ensure Email and Web services running	Web page defacement Rogue User creation Continue to services	Record activities Deliver injects	B: Email and Web functional R: Web page defaced
	<i>Reporting</i>	<i>Report status of services</i>	<i>Report level of intrusion</i>	<i>Grade B & R</i>	
Period 3	SCADA disruption Inject #3	Track down source of vulnerabilities	Disrupt runway lights and motors	Record activities Deliver injects	B: identify and mitigate R’s activities R: maintain disruption
	<i>Reporting</i>	<i>Report statuses of SCADA systems</i>	<i>Report level of intrusion</i>	<i>Grade B & R</i>	
Period 4	Chaos Inject #4	Maintain control of network	Destroy blue network	Record activities Deliver injects	B: survive R: anarchy

Given the budget constraints and as we strove to follow McRaven’s doctrine on small-scale high-precision warfare, the schedule of events was purposely packed (as shown in Table 3). Our goal for an intense schedule was to cover the major of defensive tactics that one would find in the CPT crew manual (Lee 2014). We also built into the schedule an opportunity exercise for the command and control element of a military mission. Finally the schedule contains a portion that is dedicated to helping players understand the impact of cyber on physical infrastructure. This requirement is essential to fully exercising and evaluating a Blue Team’s ability to operate in a real-world Supervisory Control And Data Acquisition or SCADA-related cyber battlespace.

Table 2 – Schedule Of Events

Time	Attacks/Actions	Tools, Tactics, Procedure	Desired Outcome
Thursday (Prep Day)	Placement of Implants	Client Side Exploit: Win 7 exploits, Java exploits Server Side Exploit: Ice Cast exploit Persistent Backdoors: NetCat exploit, Metasploit	Having the ability to gain access to the network
Friday Morning	Place Easter Eggs on the network	Example: leave a text file on the fileserver with md5 sum value of the administrator’s password	Place at least 5 flags in the blue network
Friday Afternoon	Easter Eggs hunt	Blue Team hunt the network using clues provided throughout the enclaves	Familiarization with the VITE

Saturday			
0630 – 0800	Assess environment and prep exploits	Prep work: Start MSL, Open collaboration Share Drive, Prep Exploits: Open up listeners	Ready for Period 1
0800 – 0915	Initial scan for I.P.s hostname, MAC addresses, services	Network Scanner: Nmap, Zenmap, NBtscan	Network enumerated, persistence maintained
0930 – 1115	Create rogue Users, Web page defacement	Privilege escalation: Disable UAC, “Get System” Add local and domain users. Webserver Exploit: Netcat backdoor for Webserver. Modify HTML code.	Defaced Website, rogue user created and maintained, services disrupted.
1230 – 1345	SCADA disruption	Install rogue wireless device. Make runway lights and air control tower turn off and on.	Runway and air control tower not working
1400 – 1530	Destroy Blue Network Enclaves	Delete important system files. Blue screen windows boxes. Disable Services.	All blue terminals inoperable, all critical services disabled.

INFRASTRUCTURE

The infrastructure for the exercise was very frugal. The physical hardware was four Dell servers, without any special capabilities. The software was limited to very common software including Windows 7, Windows XP, CentOS (RHEL compatible), Kali Linux, and VyOs.

Figure 3 below is a representative of the cyber battlespace. In the diagram we see two Blue Teams defending their respective “territory.” A territory is called an enclave, which is a logical network that exists and operates behind several layers protection: a router and a firewall. If comparing this to a medieval warfare scene, we would say that an enclave is a castle and the firewall is the wall and moat that protects the castle from external forces. In our exercise environment, the Red Team can be thought of as marauding barbarians, without a layer of protection.

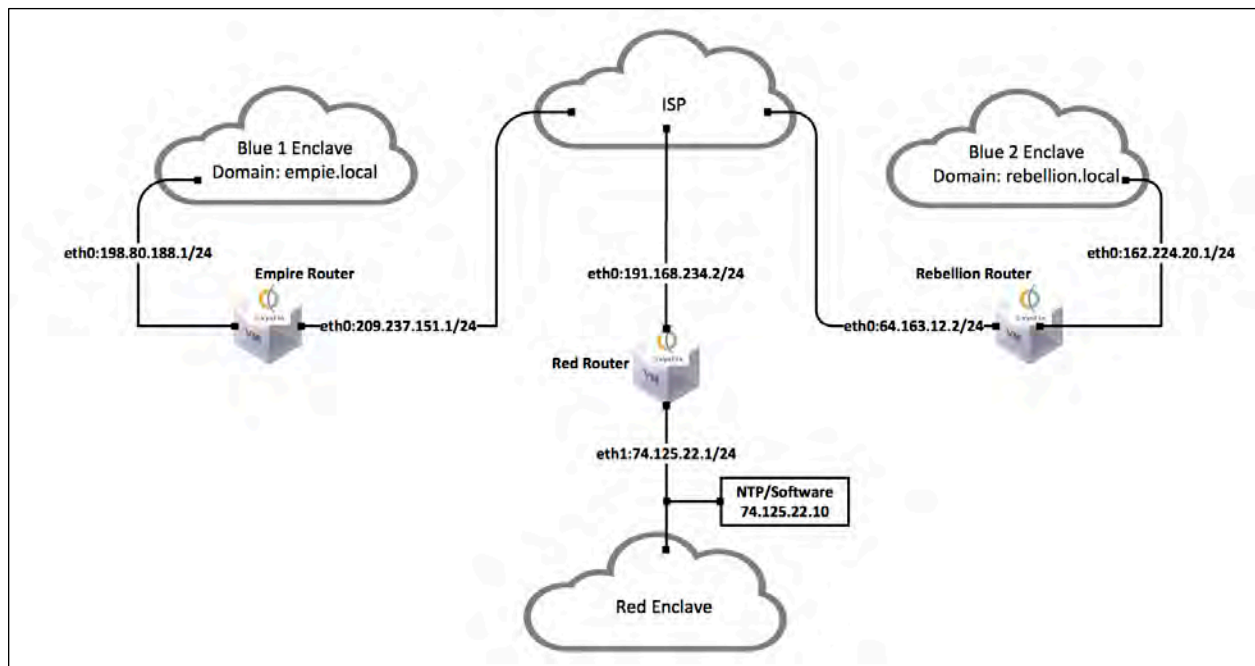


Figure 3 – Cyber Challenge Network Architecture

Within an enclave we have a number of services operating to support the life of an enclave. These include file server, email, directory, and web server. Figure 4 below is illustrative of a typical Blue enclave. One thing of note is the presence of the Human-Machine Interface (HMI) controller and the Programmable Logic Controller (PLC). These two devices are part of the SCADA model. The goal of the exercise for a Blue Team, as mentioned earlier, is to maintain all the services and exclude the Red Team. We also note that it is the PLC that can be considered to be the crown jewel. In an airport scenario, it is acceptable, albeit not desirable, if the email server and web server are not working. It is absolutely unacceptable if the runway lights and RADAR towers do not operate, as this impacts the safety and welfare of all airlines.

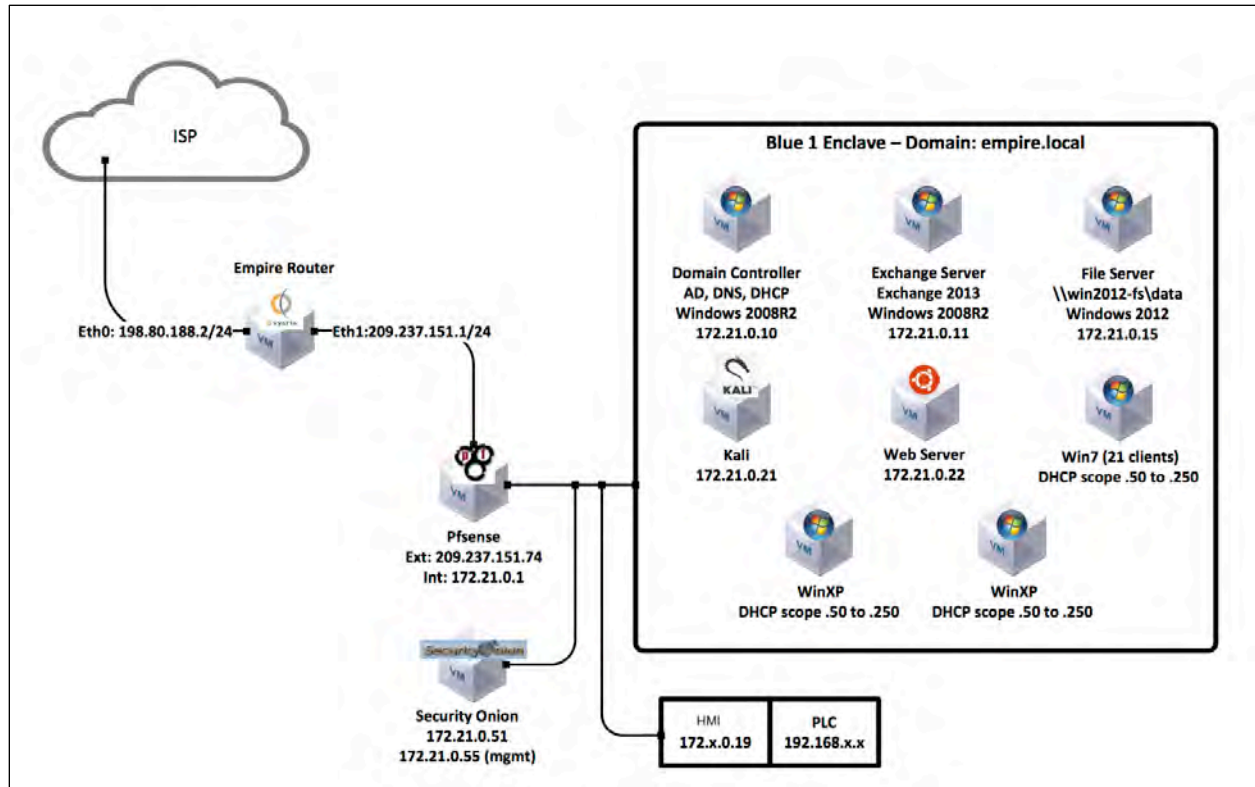


Figure 4 – Blue Network Architecture

Figure 2 shows how our partner, a National Laboratory, was able to provide a SCADA network system to give the Red Team a target. This is the sort of attack that concerns defense personnel the most. Another target is the Runway Model which would be subject to attack.

Lessons learned from our work at JFCOM on continentally-distributed simulations aided the team in producing and implementing a reliable logging capability (Graebener, Rafuse, Miller & Yao, 2003 & 2004). As these earlier, kinetic simulations were enabled by HPC to produce more and more data from more and more entities, managing the data flood became even more daunting (Yao, Ward & Davis, 2010).

ICS SCADA System

For Cyber Challenge 2015, the ICS team built a simulated SCADA system. This simulated SCADA system consisted of two runways with landing LED lights and RADAR controllers and network connectivity. The runway lights and step motors for the RADAR were controlled by a series of Arduino controllers and powered by the simulated power substation modeled by a simplified programmable logic controller (PLC) (Figure 3) provided by a national laboratory. The PLC Flyaway Kit provided the network interface to allow for seamless integration with the virtual enclave as well as logic highs and lows to control the behavior of the Arduinos and, ultimately, the runway lights and RADAR. Figure 4 shows a simplified diagram of the LED connections on the Arduino controllers.

During Cyber Challenge 2015, the Red Team attempted to disrupt the behavior of the SCADA through the PLC Flyaway Kit network interface terminal. This type of attack is an effective demonstration of the kinetic effects a hacker can have on critical infrastructure. CQRTE can connect to any SCADA system with a common network interface. This capability can provide valuable training for the SCADA engineers developing their systems and the security professionals trying to protect the systems.

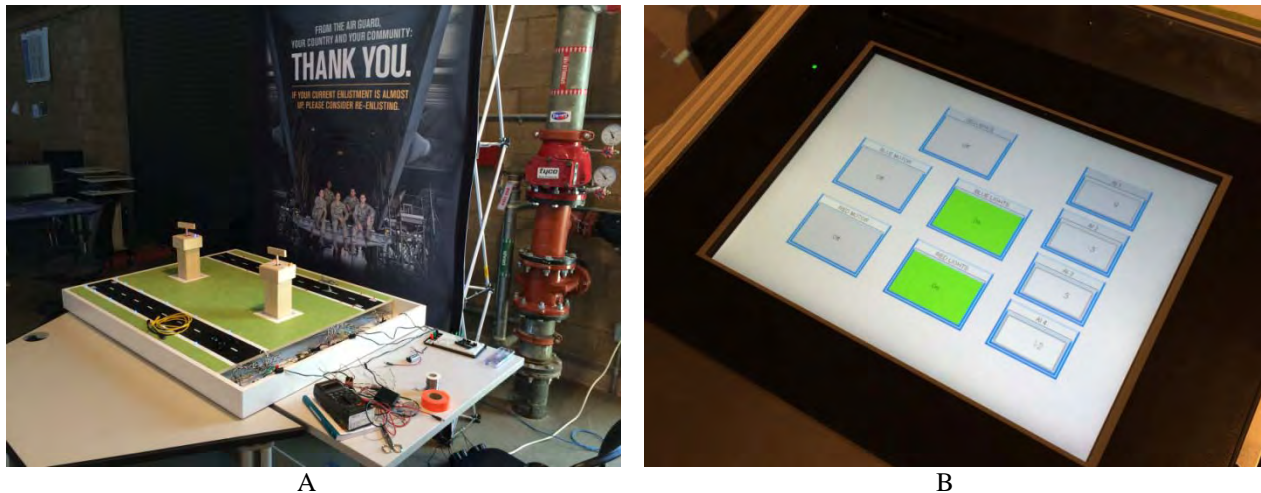


Figure 5 - (a) Dual airport runways and radar control towers, (b) PLC flyaway kit providing power to the airport runways.

In the future, to provide a more robust ICS system, the ICS team will develop a network interface using micro controllers similar to the Arduino or Raspberry Pi platform allowing for a more scalable and customized experience.

Logging Infrastructure

One of the key elements of a cyber exercise is the ability to log and to correlate exercise events and to compare them against the “ground truth.” Cyber Challenge is no different. Here, we reach out our partners at the University of Southern California Information Science Institute (USC/ISI) for assistance. USC/ISI has extensive experience providing data logging support for many of the USJFCOM’s exercises (Yao, Lucas & Davis, 2006).

The logging tools used for Windows logging are Sysmon, Nxlog, Fluentd and MongoDB. All of the Windows virtual machines in the Cyber Challenge were instrumented with Sysmon and Nxlog. The Sysmon data records detailed the Windows process events, including process creation, network connections, and changes to file creation times. Each process is given a Globally Unique ID (GUID) to allow correlation of events when the operating system reuses process IDs. Each session is assigned a GUID as well to enable grouping of events from the same logon session. These Sysmon events are stored in the Windows Event Log. Nxlog subscribes to all the events in the Windows Event Log, formats these events in the open standard JSON format, and then sends these events remotely to the Fluentd open source data collector. In our setup, there was a single Fluentd process collecting events from all Windows Nxlog processes.

The sophistication of the logging system demanded by CQRTE serves as an important indication of the necessity of collecting the “what happened.” From a science and engineering perspective, the foundation of the data logging in which we have invested a significant effort will enable our future research: answering the more challenging and higher-order knowledge “why” and “how” questions.

EXERCISE REPORT FOR CYBER CHALLENGE 2015

The actual exercise Cyber Challenge 2015 took place 6-8 February 2015 and was headquartered at the 261st Network Warfare Squadron (NWS) in Van Nuys California. Over 50 personnel participated and they were organized into five teams: (1) leadership [decision and policy makers], (2) two Blue Teams [each team is made up of Air Force and Army], (3) White Team for evaluation, (4) civilian participants, and (5) Red Team [all Air Force personnel].

The scenario was a typical model of a potentially harmful situation that would challenge national security. The scenario was predicated on a simulated major disaster in the form of a large earthquake hitting Southern California and thereby impacting the California ports and the Los Angeles International Airport (LAX) runways. Capitalizing on the calamity, two organizations “Hacktivists” [Horrendous Horde of Simi Valley aka HHSV] and the nation of “Petagonia” collaborated to hack into an emulation of the LAX's infrastructure, which was greatly simplified for exercise purposes. The Red Team placed implants into the network as a sleight-of-hand distraction, while attacking the SCADA network, which directly impacted the power substation and therefore created dangers to the runway. The Hacktivists were interested in webface defacement and other harassing tactics. The Petagonians were interested attacking the Internet Connection Sharing systems with a goal of disrupting flights thereby causing social disruption and financial damage to the United States. This is very much in accord with the types of attacks that have been witnessed in the recent past in this country.

The Cyber Protection Team is an Air Force construct which was implemented in the Blue Teams who were engaged. They were tasked with the hardening of a vulnerable network. The Computer Network Defense team is an Army construct and it performed the vulnerability assessment.

A mission set consisted of a team crew commander, who was an officer, and a battle captain, staffed by another officer. The rest of the participants were usually enlisted personnel from the Air Force or Army reserve units. For Cyber Challenge we mixed the blue-suiters (Air Force) and green-suiters (Army) and worked together to harden the systems and hunt for Red force on the network. This complies with current doctrine emphasizing joint operations. These teams were also tasked with protecting the SCADA network.

OUTCOME

As can be deduced from the data presented above, this exercise, Cyber Challenge 2015 was an outstanding success, in that it not only satisfied the goals of the proof of concept mission, it also raised the general consciousness of all of the participants and the witnesses of the opportunity for reserve units to do nationally vital work on cyber-security. These units are typically staffed with officers and enlisted who are engaged in germane professions and are committed to the defense of this country. The discovery of the utility of the reserve's intellectual assets may be one of the most valuable of all the products of this effort.

Naturally, there is a call for future use and there are emerging plans for follow-on exercises. Consideration is being made of establishing this as an annual event and including small active duty units as well. All the data management mentioned above will be needed in the future, predicated on the finding that Cyber Challenger 2015 generated 1.6 terabytes of data, all of which was logged, identified and archived.

FUTURE RESEARCH

In the short-term, we need to create a data analysis plan to review the collected data for insights and lessons learned. Longer term research goals revolve around more aggressive Red Team attacks, automatically generated scenarios, data visualization, automatically generated behaviors, and computer-assisted cyber intrusion detection. Teams are being formed to evaluate the performance of the system and procedures as fielded, as well as the appropriateness of varying metrics and analytic tools.

CONCLUSIONS

The goals of this exercise were all met and mostly exceeded our fondest dreams. The utility of the concept was clearly supported by the output of the operations personnel and the validity of the training objectives was confirmed by the positive view the participant had of the value to them. The costs in personnel time, the expenses in hardware and software, and the expenditure for travel were all minimal and mostly pre-funded in that the personnel were obligated to be on duty anyway and their compensation is planned years in advance.

ACKNOWLEDGEMENTS

The authors are grateful for the support from Richard Pace, Ms. T. Katy Bragg, and Dr. Jelena Mirkovic. We are particularly grateful to SSgt Daniel Cabrera for an excellent job done on the airport runway model, to Lt Selga for leading the Red Team, and to Major Michael “Krusty” Ehrstein for overseeing the Red force. Major Jon Dahl headed up the exercise logistics. The Blue Team leads were Capt Ammie Presley and Maj Michael Cardoza. We appreciate the tremendous support from Army’s CND commander, LTC James Parsons. Finally, we would like to acknowledge the professionalism and the contributions of all of the participants of the exercise on which this paper is based. Their service was in the finest traditions of the United State Army, of the United States Air Force and of the California Air National Guard.

REFERENCES

- Alexander, K. B. (2014). *Statement of General Keith B. Alexander Commander U. S. Cyber Command before the Senate Committee on Armed Services*. Retrieved on 12 January 2015 from: http://www.armed-services.senate.gov/imo/media/doc/Alexander_02-27-14.pdf
- Chen, T.M. (2013). *An Assessment of the Department of Defense Strategy for Operating in Cyberspace*, Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, September 2013
- Clark, Ben (2014). *The Red Team Field Manual (RTFM)*. CreateSpace Independent Publishing Platform.
- Cyber Flag, (2013). *Cyber Flag Exercise Highlights Teamwork, Training*, Retrieved on 12 January 2015 from: <http://www.defense.gov/news/newsarticle.aspx?id=121179>
- Cyber Guard (2014). *Cyber Guard Exercise Tests People, Partnerships*. Retrieved on 13 January 2015 from: <http://www.defense.gov/news/newsarticle.aspx?id=122696>
- Cyber Shield (2014). *Cyber warriors flex digital muscle at 2014 Cyber Shield exercise*. Retrieved on 13 January 2015 from: <http://www.nationalguard.mil/News/ArticleView/tabid/5563/Article/8972/cyber-warriors-flex-digital-muscle-at-2014-cyber-shield-exercise.aspx>
- Gottschalk, T. D., Lucas, R.F., Yao, K-T., Wagenbreth, G. & Davis, D. M., (2010), Distributed and Interactive Simulations Operating at Large Scale for Transcontinental Experimentation, in the *Proceedings of the IEEE/ACM Distributed Simulations and Real Time Applications 2010* Conference, Fairfax, Virginia
- Horowitz, S., Orlansky, J., Tillson, J.C.F., Gemelas, T.C., Gillman, H.J., Hammon, C. & Hoyler, H.M. (1995), *Unit Training in the Gulf War*, IDA Paper P-3087, Institute for Defense Analyses, Alexandria, Virginia.
- Jean, G.V. (2006), *Game Branches Out Into Real Combat Training*, appearing in National Defense, Retrieved from: http://www.nationaldefensemagazine.org/archive/2006/February/Pages/games_brance3042.aspx on 10 February 2015
- Lee, L. (2014) *Cyber Protection Team (CPT) Crew Operations Manual*. Unpublished internal manual, Johns Hopkins Applied Physics Laboratory, Laurel, Maryland.
- Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Rand Corporation.
- Lucas, R., & Davis, D., Joint Experimentation on Scalable Parallel Processors, (2003), in the *Proceedings of the Interservice/Industry Simulation, Training and Education Conference*, Orlando, Florida, 2003

- Lynn, W. J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, 97-108.
- McRaven, W. H., (1993), *Theory of Special Operations*. Master's Thesis, Naval Postgraduate School, Monterey, California.
- Po'oihe (2013). *Hawai'i National Guard, University of Hawai'i conduct large scale cyber-range exercise*. Retrieved on 14 January 2015 from: <http://dod.hawaii.gov/blog/in-the-news/hawaii-national-guard-university-of-hawaii-conduct-large-scale-cyber-range-exercise/>
- Scavo, C., Kearney, R. C., & Kilroy, R. J. (2008). Challenges to federalism: Homeland security and disaster response. *Publius: The Journal of Federalism*, 38(1), 81-110.
- Schneider, S. K. (2005). Administrative breakdowns in the governmental response to Hurricane Katrina. *Public Administration Review*, 65(5), 515-516.
- Tran, John (2014). *Prometheus's Fire or Pandora's Box: Formalizing Cyberspace Planning Process*. Air University. Maxwell AFB,
- U.S. Congress (1995). *Distributed Interactive Simulation of Combat*. OTA-BP-ISS-151, Office of Technology Assessment, Washington, DC: U.S. Government Printing Office.
- van Riper, P.K. (2004), *The Immutable Nature of War*, Interview transcript recorded by NOVA, the Public Broadcasting System, Retrieved from: <http://www.pbs.org/wgbh/nova/military/immutable-nature-war.html> on 10 February 215.
- Yao, K-T., Davis, D. & Lucas, R. (2006). Supercomputing's Role in Data Problems and Its Contribution to Solutions, *The ITEA Journal of Test and Evaluation*, Fairfax, Virginia, Sep-Oct, 2006.
- Yao, K-T., Ward, C. E. & Davis, D. M., (2010), Data Fusion of Geographically Dispersed Information: Experience with the Scalable Data Grid, in the *Proceedings of the ITEA Annual Technology Review*, Charleston, South Carolina