Dynamic Cybersecurity Training Environments for an Evolving Cyber Workforce

Vincent E. Urias, Brian Van Leeuwen, William M.S. Stout, Han W. Lin
Sandia National Laboratories
Albuquerque, New Mexico, USA
{veuria,bpvanle,wmstout,hwlin}@sandia.gov

***Abstract*—A cybersecurity training environment or platform provides an excellent foundation tool for the cyber protection team (CPT) to practice and enhance their cybersecurity skills, develop and learn new knowledge, and experience advanced and emergent cyber threat concepts in information security. The cyber training platform is comprised of similar components and usage methods as system testbeds which are used for assessing system security posture as well as security devices. To enable similar cyber behaviors as in operational systems, the cyber training platforms must incorporate realism of operation for the system the cyber workforce desires to protect. The system's realism is obtained by constructing training models that include a broad range of system and specific device-level fidelity. However, for cyber training purposes the training platform must go beyond computer network topology and computer host model fidelity - it must include realistic models of cyber intrusions and attacks to enable the realism necessary for training purposes. In this position paper we discuss the benefits that such a cyber training platform provides, to include a discussion on the challenges of creating, deploying, and maintaining the platform itself. With the current availability of networked information system emulation and virtualization technologies, coupled with the capability to federate with other system simulators and emulators, including those used for training, the creation of powerful cyber training platforms are possible.**

I. Introduction

Currently, there are no standardized concepts or methods for offering cyber training. This holds true across all sectors currently offering cyber training, although available literature shows multiple recommendations to develop and implement standards [1][2]. The need for effective cyber training increases in tandem with the need for security professionals. The Frost & Sullivan's 2015 $(ISC)^2$ Global Information Security Workforce Study [3] estimates a global shortfall of 378,000 information security staff, a figure that is projected to increase to 1.5 million by 2019. The available training programs emphasize real-world scenarios and an informed attack-based approach (to be offensive and understand the adversary), while remaining defensive of the network. An effective attacker needs to know more about the defensive teams operations and systems than they do and defensive cyber teams must also have a good grasp of the adversary and the adversarys methods [4].

In secure computing operating environments, custom-made testbeds are often created from real hardware components and are used to assess impacts of security breaches or evaluate strategies for deployment of new security capabilities. These single-purpose testbeds are expensive, difficult to maintain, and time-consuming to construct and deploy. An alternative is the use of modeling and simulation to answer system security questions. In most cases, simulation models do not exist; either simulation model code needs to be developed to simulate the devices in question or extensions made in order to answer specific questions. It is our belief that instead of single-purpose or simulation testbeds, system testbeds with variable fidelity environments used for assessing system security can also serve as the basis for training system defenders; these Live, Virtual and Constructive (LVC) environments can be made to effectively represent operational systems, and even adversaries.

We begin this position paper by first covering current training methodologies. We then delve into the benefits of leveraging LVC to produce training environments that can be deployed on-the-fly; in this section we also cover system requirements, as well as perceived gaps, limitations and opportunities with such training approaches. Using some of the tenets we outline, we then explore a use-case of deploying an LVC-based training scenario. In the final section of we conclude our paper.

II. Current Methods and the Status Quo

There are two distinct roles where it becomes increasingly important for individuals to have well-developed, highly realistic training: first responders and cybersecurity practitioners. It is not enough to evaluate the readiness of cyber and first responders based on professional certifications it is necessary to provide a training environment that matches the ultimate objectives of the engagement and is critical that there is a way to evaluate the actions taken by the trainees to determine areas of strength and weakness, which can lead to additional training to address any deficiencies in capability [1]. The professionals charged with defending the nations networks and services must receive training in the skills required to be successful, but must also be able to navigate potential high-pressure, combative environments. All cyber training should constantly link back to the impact on operations (both our own and the adversary) [4]. Pilots and soldiers receive this sort of training and it needs to be carried over to the cyber domain as well.

Several organizations, such as the Defense Information Systems Agency (DISA), have established cyber training courses, such as Department of Defense Information Networks (DoDIN) Cyber Protection Team (CPT) cyber readiness squad

978-1-5090-6356-7/17/$31.00 ©2017 IEEE

courses for networks, Windows systems, security analysis, and the Host-Based Security System (HBSS) [8][9]. Additional courses focus on active directory, network protection, and patching methodologies. However, these training environments are limited to the noted areas and lack training support for active protection of systems. In some cases, training objectives are met through targeted cybersecurity exercises rather than actual training programs, making it difficult to find a way to ensure that professionals are receiving the appropriate training to increase their skill sets and to evaluate the readiness of their skillsets. Cyber pedagogy is being influenced more by exercises than by textbook topics; consider the Cyber Defense Exercise (CDX) [5]. Students that find themselves in communication-related fields benefit from experience in designing and implementing networks. Students that find themselves in cyber-related fields will benefit from experience in network attack and defense. But ultimately, all of the students benefit from being part of the entire process.

Although there are no standards for delivering cyber training, a high percentage of the training programs currently being offered in academic, government, and private sectors rely heavily on virtualization. Virtualization has long been accepted as an effective way to provide realistic training environments that are low-cost, easily reproducible, safe, and encourage exploration and breaking with an easy way to reset [6][7]. Even though most training providers have incorporated virtualization into their curriculum, there are still many different ways to do so. It is our opinion that cyber practitioners need more than they are getting today. Capture the Flags (CTFs) are not enough, SANS is not enough, Red+Blue may be limited, and existing environments may not provide the ability to address actions in realtime, record events, introspect or observe the students without introducing artifacts into the system. We believe leveraging LVC with a Cyber Defense Exercise mentality provides a vast malleable platform to meet multiple cyber training objectives.

III. The Benefits of Live Training

A cybersecurity training environment provides an excellent foundation for cyber CPTs to practice and enhance their cybersecurity skills, develop and learn new knowledge, and experience advanced and emergent cyber threat concepts in information security. The cybersecurity training environment may be categorized as static or dynamic. Static training is often built by constructing a predefined set of learning objectives into virtual machines. This approach is very effective but not adequate in preparing hands-on training for CPTs in a realistic contested cyber environment. In severely contested cyber environments, there may be multiple attack vectors, adversaries and adversarial objectives. The adversaries are free to innovate tactics against the CPT as they see fit. There will not be a set of scripts or a concept of operations (CONOP) for the CPT to follow. This requires a dynamic and realistic environment be constructed for the CPT to train or exercise in.

Dynamic training environments provide realism and true-to-life scenarios where trainees/CPTs have the opportunities to work together synchronously as a team. This is particularly useful for an effective cyber defender; the CPTs need to observe, evaluate, decide and act quickly so that cyber exploits are minimized. In addition, dynamic training environments amplify learning experiences by simulating complex scenarios that can enhance the CPTs understanding of the global view of the cyber threats. Finally, such environments may promote realism and provide hands-on opportunities for success and failure without risk to operational systems.

A. Cyber Training Platform Requirements

Cyber training platforms must incorporate realism to enable similar cyber behaviors as operational systems the cyber workforce desires to protect. The system realism is obtained by constructing training models that include a broad range of system and specific device level fidelity. For cyber training purposes the system level fidelity must go beyond computer network typology and computer host models and must include models of cyber intrusions and attacks to enable the realism necessary for training purposes. A key aspect in constructing the modeled systems is to include the range of diversity of devices that comprise operational systems of interest. When developing cyber training platforms models the analyst must consider incorporating fidelity in the following system aspects:

1) Hosts: The computer network replicated in the cyber training platform should include models of workstations and servers. Additionally, some training objectives may require networks that include devices such as network printers and communication devices (e.g., VoIP telephones). Fidelity in the hosts should include faithful representation of the operating system and host-based security. The training objectives may also require hosts to incorporate mission critical application software and enterprise services such as domain controllers.

Additionally, with the proliferation of networked mobile devices cyber training may require representations of this connectivity. This connectivity may be enabled by private networks such as WiFi or may be enabled by third-party infrastructures. Representing these components can pose significant challenges; however, abstractions to the connectivity may be adequate for the specific training objective.

2) Network system architecture: The computer network architecture should be represented with fidelity consistent with training objectives. Typical training objectives include identifying intrusions resulting from connectivity to public networks (e.g., Internet). Thus faithful representations of network firewall locations and DMZ implementations are important. Location in the network of enterprise services should be represented and configurations of VLANs and access control lists controlling network reachability must be represented in the model.

The training platform should have the capability to support models of varying scale. Some training objectives can be achieved with reduced scale models that include system components necessary to represent cyber intrusions without a

978-1-5090-6356-7/17/$31.00 ©2017 IEEE

full-scale replica. The training objective will drive the scale needed for the training. Network models should have fidelity in network devices, such as routers and switches, if the training includes intrusions that are dependent on specific manufactures and operating systems.

In cases, specific network protocols are necessary for the training objective. An example is IPv6-enabled networks. IPv6 incorporates a suite of network mechanisms and protocols that creates opportunity for classes of cyber-attacks not found on IPv4 networks. Another example is the mechanisms and protocols associated with mobile communications that are integrated into an enterprise computer network system.

3) System security mechanisms and applications: Security software plays an important role in the defensive of computer network systems. Security software are the sensors of the system and provide the necessary data for a security analyst to understand the security posture of the system. The security analyst must train on system models that include the same sensors or similar class of sensors deployed on the operational system of interest. Thus, the cyber training platform must have capability to model the range of security mechanisms and provide mechanisms that present the data to the analyst. An example of the range of security mechanisms used in securing a computer network system ae those used in the Security Onion [10].

4) System load and network traffic: The overall computer network system the training environment intends to replicate has a specific purpose. This purpose may be an enterprise computer system supporting various business aspects such as operations and finance. The system could be a SCADA system supporting the distribution of electrical power. In either case, the cyber training platform should replicate the purpose and types of applications that fulfill the purpose the system. The applications interact with other applications and services throughout the system and other systems including those on public networks. The system loads and traffic should be modeled to provide similar types of legitimate traffic to the security sensors. The level of fidelity is dependent on the training objective.

5) Malicious intrusions and cyber-attacks: A key, and potentially a very challenging part of a cyber training platform is the capability to produce malicious activity on the modeled system. This part requires the modeling of cyber-attacks to provide the computer network system behaviors the training parties attempt to identify and mitigate. Classes of attacks and specific attacks in those classes can be found in cyber-attack taxonomies [11]. Additionally, attack models can be constructed from data obtained from real-life cyber incidents.

The above criteria lays a foundation for the required fidelity a computer network system model must include to enable cyber training. Additional attributes a cyber training platform must include are:

- *Data collection for evaluating the training results.* Cyber workforces that use the training platform should receive feedback on their effectiveness and skill at thwarting intrusions and attacks. Feedback should be provide to the cyber workforce to identify strengths and weaknesses and identify what actions were effective at thwarting acts (and what actions were not effective). The training platform should incorporate methods or algorithms for scoring and measuring the effectiveness of the approaches, tactics, and techniques the defender employed.
- *Ease of setup and cost.* How quickly and cost effectively can experiments be designed and implemented (i.e., machine speed vs. human speed)? Computer network systems and cyber-attack techniques are in constant change and training platforms must have flexibility to reflect present-day scenarios without incurring prohibitive costs.
- *Geographical and temporal persistence.* The cyber platform should be deployed and hosted in such a way that it may be accessible from any geographical location and at any time. This notion of persistence allows one or many teams the ability to train together throughout the year, not just during annual exercises/events.
- *Validation and verification.* A major challenge in employing models of operational systems is the validation and verification of the model. Approaches and mechanisms should be used to identify the accuracy of the models used in the cyber training platform.

B. Perceived Gaps, Limitations and Opportunities

Dynamic training environments have the capacity to provide high-fidelity playgrounds where cyber practitioners, either novice or experienced, may have the opportunity to build or hone their skills. However, the perception may be the environments themselves may yield a less than desirable return on investment. Some of the arguments against such training environments include:

"Training environments do not adequately represent operational systems." While this argument may hold for large, physical systems/processes that cannot be represented in simulation, in a cyber context virtualization is sweeping away the former physically-confined aspects of enterprises.

"Training environments are often stuck in the contexts they were developed in and stale quickly." To refute this claim it is necessary to consider the input interfaces to the primitives of the training the system. Live data, historical data and generated data can all be used as input to a system to provide the ability to refresh, update or enable dynamism in the training environment.

"System maintenance of a virtual training environment is too much work." Through system deployment automation and instrumentation for automatic feedback, the systems can be specified and simply updated to reflect changes as required. Also, since the environment and its components are modular (e.g., virtual machines), elements may be updated, added or completely removed with little to no impact on the rest of the system.

No solution is simple in and of itself, but through carefully consideration of the options and technology available, paths forward readily present themselves. The catch is that the methods to support dynamically mutating the environment

978-1-5090-6356-7/17/$31.00 ©2017 IEEE

should be integrated into the system not as an additional feature, but as a required functionality within the system itself. Leveraging techniques often found in cloud resource allocation, virtualization, software defined infrastructures, and dynamic system specification provide more than adequate tools to effect the changes needed to support the solutions. In this context, it is necessary that designers of the training platform consider the integratability, interoperability and composability of the system. The first deals with bringing physical and virtual systems together; the second, with interfaces (software and/or hardware) to adequately transfer data elements between components; the final addresses the ability to modularize and construct environments effectively [12][13].

One of the greatest advantages that comes with the design and implementation of a full-scale live training environment is the ability to apportion out parts of the system to unique applications. This speaks to the modularity and multimodality of the system. For example, the system can be apportioned to meet smaller tasks such as:

- Appliance training: As new appliances or devices are brought into the network, burn-in, performance or operational testing may be performed. Such an application might include testing the security or performance features of a device to ensure it meets specifications or won't impede other network functions, or for operators/maintainers to familiarize themselves with the device in a non-operational environment.
- Specific task reinforcement: If a simple task is needed to accomplish something larger, a smaller, focused interaction may be used. For example, if a practitioner needs training on reviewing log files or document features, then small containers or virtual machines may be used to interact with such items; the containerization of the items lends itself to repeatability and the ability deploy the training individually with expediency.
- Targeted scenarios: When many specific tasks collude to form a scenario, a small-scale demonstration environment may be deployed for practitioners to interact with. For example, if a student needs to employ tool sets or applications to examine activity, features or behaviors from devices or actors on system(s), training enclaves may be used; the enclaves may be customized to allow one or more students to be engaged.
- Certification/technique training: Some work environments (e.g., floors) require system certification or qualification testing of practitioners to be allowed to work in the operational context. The flexibility of a dynamic training environment allows training and exam developers the ability to modularize tasks and scenarios and combine them for topical examinations that may be customized for the role the practitioner will play. Instrumentation of the environment can provide instant feedback on the actions of the student in realtime.
- Team studies: Custom environments may be deployed that replicate portions of operational systems that may be prone to attack. Using system inputs (system logs, VNC replay, packet replay, etc.), these environments may be used to reduplicate the actions of known attacks, or even the action of successful defenders. The reenactments can be used to provide studies of actors or defenders to students (even decision-makers and customer too) to provide system views, context, and immediate visualization of what cyber defense and attack look like.

The ability to fuse these examples together under the umbrella of a consolidated training environment can also provide sequenced or process-based training opportunities. Also, with defined module interfaces, the ability to stretch training between logically and geographically divergent areas also becomes a possibility. One may see the benefits for this as not only maintaining consistency of a trained force across a latitudinally spread enterprise, but also as a synergistic environment that can be used between companies or agencies to share current approaches to security, tools, and techniques used to combat the most recent threats and actors.

IV. Use-case Example and Lessons Learned

For many years, Sandia National Laboratories has been developing customized tools and technology to implement realistic enterprise models and emulations with device diversity comparable to operational systems. The developed platforms include instrumentation, data collection, and backend analysis capabilities that ingest structured and unstructured data from the network, applications, hosts, and network defense tools to enable key aspects of the training and post-training analysis.

To test our LVC training concepts, Sandia partnered with an external customer to create a customized training environment to exercise our training methodology and platform. The primary objective of the environment was to train teams to *fight through*, focusing particularly on network defense and hunt. The environment consisted of both physical and virtual assets, as prescribed by the customer in order to develop a realistic landing and playground the students were familiar with and could interact with. A network view of the simulated topology prior to deployment is shown in Figure 1. The following sections describe the platform itself, deployment of high-fidelity attributes, and the collection of relevant data from the experiment.

A. Training Environment and Topology

To support the training objectives, three training zones were developed. Two zones α and β were located at Sandia, the third zone, γ at the customer's location. The network defense teams were introduced into the environment from a shared topology in γ-zone. The α-zone emulated a DMZ security stack that consisted of routers, firewalls, an intrusion-detection-system (IDS), and enterprise services (DNS, email, web). Physical devices were also incorporated in this zone, intentionally misconfigured and/or with security vulnerabilities to facilitate hunt endeavors, and exercise exploitation discovery and/or response. The β-zone bridged both the α and γ zones and consisted of a virtualized global Internet, an

978-1-5090-6356-7/17/$31.00 ©2017 IEEE

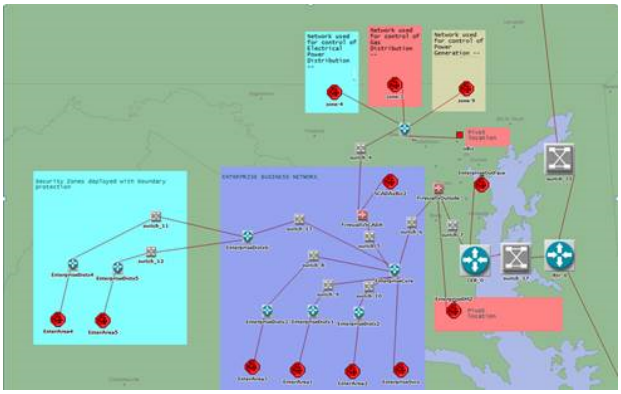

Fig. 1. ICS and Enterprise Topologies (β-zone).

Industrial Control System (ICS), and an Enterprise network. All three zones were logically connected as one seamless virtual/physical environment to exercise the teams skills of reconnaissance, exploitation/remediation and pivoting.

Sandia and the geographically separated customer site were physically connected via dedicated a virtual private network (VPN). Using Layer2 tunneling protocols, team workstations from the γ-zone at the customer site were brought directly into the virtual global Internet, occupying virtual workstations in the landing network enclave. Team members were free to explore all of the environments and exercise their skills.

B. High-Fidelity and Interactivity

In order to create a realistic, representative and high-fidelity environment, physical/virtual devices, application services and traffic generation were integrated and interfaced at varying physical and logical layers. Requirements were drawn from example topologies derived from training curricula and trainer/Subject Matter Expert (SME) inputs; those requirements were then manifested through specific service applications (hosted on virtual machines (VMs)), physical devices, and device/service configurations (e.g., firewalls, routers). Through software stubs and emulation platform scripting, configurations were injected at environment boot-time into the VMs to instantiate and configure the selected applications.

To represent network infrastructure, virtual/physical routers, Layer2 and Layer3 switches were instantiated within the environment. The devices were configured not only to provide connectivity and routing, but also apply Quality-of-Service parameters to emulate network realism (e.g., routing protocol broadcasts, network delay). To represent endpoints and servers, the emulation platform itself provided the instantiation of the VMs through *snapshot*, or through *write-back* as required. The former may be used for "throw-away" VMs to support high-density experiments, while the latter imports the need to capture and record changes made to or actions done within the VM. Either VM instantiation method allows unique configuration through the use of techniques like virtual disk image file insertion, out-of-band network configure protocols, DHCP and also device-specific in-band configuration methods. Applications in the environment consisted of common server-based services such as instant messenger, collaborative bulletin-boards, cyber defense tools, and web servers. To facilitate training objectives, exploitable VM targets were added to the network for hunting, pivot points, and for remediation exercises in the multi-day event.

To promote interactivity in the environment, we leveraged the ability to add/remove VMs and services at will: VMs were added with graphical user interfaces that allowed opposing team members or instructors to interact with trainees on-the-fly. Artificial interactive means were also employed; techniques such as framebuffer-replay [14] were used to emulate actions on endpoints to represent users, or to generate machine-to-machine communications. Platform traffic generation utilities were used between endpoints to "fill-the-pipes" with HTTP/S, email, and secure-shell traffic.

C. Data Collection

In training environments, the need for effective feedback and grading mechanisms are dire for the evaluation of the trainees, and for the further development of pertinent training objectives. Thus, the training environment must be flexible and configurable with respect to data output; data extraction and collection must also pay mind to formatting and normalization, to ease the parsing and ingestion requirements for analytic applications. Our employed emulation platform provided the following capabilities: (1) introspection on virtual machines from the hypervisor; (2) capture of point-and-click type operations from user Virtual Network Computing (VNC) based sessions; (3) collection of network flow traffic and full-packet capture on the physical host machine virtual switches.

The virtual network devices deployed in the environment provided for network monitoring applications to poll Simple Network Management Protocol (SNMP) data (e.g., performance metrics, routes, switching table entries). Endpoint VM workstation instantiations included agents to query and push host data to collection servers in- and out-of-band. Additionally, agentless introspection tools were connected via the platform's VM hypervisor to monitor specific actions done on the endpoints. This latter technique was particularly advantageous for hunting operations that would disable monitoring agents installed on the VMs.

Network monitoring applications were tooled to ingest active and passive network data to generate general and customized reports. Network data was also fed to the primary analytic engine that receive VM host data via VM agents, hypervisor-based introspection, and in-experiment virtual machine services (e.g., firewalls, IPS, etc.). Collectively, the fusion of the many data sources provided a rich view into the system throughout the course of the training scenario; the level of granularity could be made coarse for high-level discourse or fine-grained for detailed analysis.

D. Lessons Learned and Future Research

Several lessons were learned in creating realism within the environment and the effects/rewards of realtime monitoring

978-1-5090-6356-7/17/$31.00 ©2017 IEEE

and introspection for instant feedback generation or deferred analyses. Using the data collection techniques deployed in the environment, Sandia was able to capture the customer's team's movements through the virtual and physical networks. Collection not only revealed their actions from the networking perspective, but also on host as granular as the mouse points, clicks and keyboard entries on the virtual machines. Furthermore, the capture of network packets, binaries executed on endpoints, and VNC replay of actions done on endpoints provided much context about the actions of the team members. So, while instrumentation may provide a great deal concerning the "whats" of the training exercise, extrapolation to other areas of question were less understood and provide fodder for future areas of research.

Collected data may provide fine-granularity of specific events in time; events may be stitched together loosely to provide some assumption of actions occurring sequentially. However, the true meaning behind actions taken and the full residual effects were difficult to deduce. That is, event correlation between a few or many seemingly disparate events with causality analysis is difficult to pin down. An analogy can be made to keys typed on a keyboard that in turn affect an application's configuration that in turn may produce some cascading effects to other objects. Working backs from those other objects is difficult; deducing future effects based on previous effects is difficult; finding and understanding underlying motivations is difficult.

Another perceived challenge exists in the emulation of the "cyber cockpit." As in simulation training modules, students may be taken through a course of events that bring them to decision branches in the training sequence. If a student fails to respond appropriately at an instance χ, the simulation may be reverted back to that instance χ for remedial/reinforcement training. In a live training environment, such decision points must be readily understood beforehand and injected into the environment at the appropriate instance or location - not unlike a gaming engine that must reason based on user inputs and either restart, resume or end the scenario. Further research in the this area may also delve into understanding, capturing and reacting to behaviors with social/psychological analyses.

The final area we observed was the need to develop appropriate Measures of Effectiveness (MOE). The training teams would have to understand their roles, tasks, and how their actions supported (or impacted) overall mission. The need then is to tie those MOEs that determine "mission accomplishment" against tests and objectives deployed in the training environment. The need is further made complex by not only developing the pertinent and correct metrics for individual MOEs, but also team-based MOEs. These measures are also detrimental to the goals of implementing policy, developing TTPs, assessing/analyzing information, and reporting functions back to trainers.

V. Conclusions

There is a need for a foundation tool for CPTs to practice and hone their cyber skills, develop and learn new knowledge, and experience advanced and emergent cyber threat concepts in a realistic training environment. "Train as you fight is applicable to the cyber warrior, just as it is to the solder on the ground. While the practical experience gained from using physical training environments is high, there are many difficulties with deploying and maintaining such environments. In this paper we discussed the benefits, challenges, and design issues with leveraging LVC for cybersecurity training platforms, to include: integral components and technical requirements of an LVC-based training platform; applicable approaches to create training scenario topologies; deployments using network/compute virtualization and emulation techniques. It is our opinion such approaches are the path forward to better train and equip an ever evolving cyber workforce.

We closed our paper with the details of a customer supported LVC training exercise. The example training scenario illustrated the realism obtainable with a LVC approach that would not be not possible with alternative static/physical approaches. The results demonstrated how a training platform can significantly enhance the teaching process of cybersecurity of networked systems, and uncovered interesting but necessary areas for future research.

References

[1] J. Yoon, S. Dunlap, J. Butts, M. Rice, B. Ramsey, "Evaluating the readiness of cyber first responders responsible for critical infrastructure protection," International Journal of Critical Infrastructure Protection, Volume 13, June 2016, Pages 19-27.

[2] V. S. Harichandran, F. Breitinger, I. Baggili, A. Marrington, "A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later," Computers & Security, Volume 57, March 2016, Pages 1-13.

[3] M. Suby, F. Dickson, Frost & Sullivan, "The 2015 $(ISC)^2$ Global Information Security Workforce Study," A Frost & Sullivan White Paper.

[4] D. J. Clark, "An onion approach to cyber warfare training," 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, 2015, pp. 1-4.

[5] B. E. Mullins, T. H. Lacey, R. F. Mills, J. E. Trechter, S. D. Bass, "How the Cyber Defense Exercise Shaped an Information-Assurance Curriculum," in IEEE Security & Privacy, vol. 5, no. 5, pp. 40-49, Sept.-Oct. 2007.

[6] S. D. Burd, C. Conway, A. Seazzu, "Virtual Computing Laboratories: A Case Study with Comparisons to Physical Computing Laboratories," Journal of Information Technology Education: Innovations in Practice, vol. 8, pp. 55-78, 2009.

[7] S. D. Burd, X. Luo and A. F. Seazzu, "Cloud-Based Virtual Computing Laboratories," 2013 46th Hawaii International Conference on System Sciences, Wailea, HI, USA, 2013, pp. 5079-5088.

[8] DISA, Cyberworkforce Development, http://www.disa.mil/Initiatives/Cyber-Workforce-Development, 2017.

[9] DISA, "Cyber Protection Teams are "New Infantry" says Hickey," http://www.disa.mil/NewsandEvents/2016/Hickey-Cyber-Protection, 19 September 2016.

[10] Security Onion, https://securityonion.net, 2017.

[11] Mitre, Common Attack Pattern Enumeration and Classification: A Community Resource for Identifying and Understanding Attacks, https://capec.mitre.org/, 2017.

[12] E. H. Page, R. Briggs, J. A. Tufarolo, "Toward a Family of Maturity Models for the Simulation Interconnection Problem," Proceedings of the Spring 2004 Simulation Interoperability Workshop, IEEE CS Press.

[13] A. Tolk, "Interoperability and Composability." Chapter 12 in J.A. Sokolowski and C.M. Banks (Eds): Modeling and Simulation Fundamentals - Theoretical Underpinnings and Practical Domains, John Wiley, 403-433

[14] T. Richardson, J. Levine, Internet Engineering Task Force (IETF), "The Remote Framebuffer Protocol," IETF Request for Comments: 6143, March 2011, https://tools.ietf.org/html/rfc6143, 2017.

978-1-5090-6356-7/17/$31.00 ©2017 IEEE