Cyber Range Optimization: Advanced Tools for Advanced Defense

Reid Stosik
reidsto@mail.regent.edu
Young B. Choi
ychoi@regent.edu
Department of Engineering & Computer Science
Regent University

Abstract

The lag in preparedness to thwart malevolent assaults in cyberspace on governments, utilities, businesses and citizens is evidenced by the fact that "it takes on average 146 days to detect a malicious attack in an organization's environment" (Zakhour, 2016). In 2016, 87% of the private sector reported incurring at least one cyberattack. The toll on American business enterprise is one that affects every American consumer and the GDP. As big data gets bigger daily, cybersecurity is challenged minute by minute to protect organizations of every kind from frequent, complex threats. This study provides a brief overview of the recent evolution of cyber ranges, a shift from the predominantly classified arena into the unclassified, of the superiority of cyber ranges over audits and simulation for cybersecurity effectiveness and provide examples of cyber range optimization and their advanced tools for advanced defense of organizational assets--ultimately demonstrating that cyber ranges are significant, if not essential components, in both public and private sectors for advanced defense in a hostile environment.

Keywords: Cyber Range, Cyber Range Optimization, Advanced Tools, Advanced Defense, Cybersecurity

Introduction

A cyber range is a virtual environment used for cyber warfare training. It provides tools that help strengthen the stability, security and performance of cyber infrastructures and IT systems. The cyber range and its warriors (IT professionals) train, develop and test themselves and their system technologies to ensure readiness in all sectors for real world cyber combat. Cyber range architecture generally falls into three categories, 1) physical—duplication of entire physical network infrastructure--switches, routers, firewalls, servers, endpoints, etc. for training, 2) virtualized--components are emulated with virtual machines, and 3) hybrid—engages virtual elements when and where they make sense, mixing physical elements when and where they make sense. Generally, the hybrid solution provides the best balance of cost performance and scale when building an optimal environment to train cyber warrior assets and evaluate network resiliency:

"The hallmark of a good cyber training exercise is realism. You may have a beautifully designed hybrid range, but if the right types of realistic background, your mission-critical network traffic, aren't flowing to match your real-world scenarios, and if you can't generate mono-realistic attack patterns at high scale, then you aren't training as you fight" (Ixia, 2014).

A first step toward equipping an organization to make complex technology assessments is a well-designed cyber range, giving corporate cyber warriors a fighting chance against today's creative cyberterrorists. Cyber range optimization includes a hybrid physical/virtual constructed with application and security test tools to facilitate realistic ratios of highly-scalable, mission-critical background and attack traffic, simultaneously, supplying detailed, real-time analyses with comprehensive reporting tools.

Evolution of Cyber Ranges

Saadawi and Jordan (2011) provide insight into catalysts for the development of cyber ranges: "Unfortunately, as our [technology] dependency has grown, so have hostile attacks on the cyber infrastructure by network predators. The lack of security as a core element in the initial design of these information systems has made common

desktop software, infrastructure services, and information networks increasingly vulnerable to continuous and innovative breakers of security" (v).
From a U.S. perspective, new concepts and initiatives emerged from the Comprehensive National Cyber Initiative (CNCI) in March 2010, which recommended that the government "must incorporate a creative and aggressive cyber 'opposing force' to stress the system in future experiments and exercises" (2011, 19).

In an effort to advance security as a priority, it was announced in 2011 that the U. S. Department of Defense, in cooperation with key private sector partners including defense contractor Lockheed Martin and Johns Hopkins University in Maryland, was building "a 'scale model' of the Internet to carry out cyber war games. This system was designed for "researchers to simulate attacks by foreign powers and from hackers based inside the U.S." This precursor to cyber ranges (both classified and unclassified) was developed by the Defense Advanced Research Projects Agency (DARPA), whose early network research was integral to the development of the Internet. After the agent.btz worm infected the military network in 2008, President Obama declared cyber threat one of the country's most serious challenges (BBC, 2011). The National Science Foundation and DARPA invested well over $110 million dollars in the Orlando-based cyber command center that was restricted to those in the "top secret" domain (Wood, 2013). According to cyber jihad expert, James Scott, "The US Cyber Command is 'DDoSing' ISIS servers, taking down social media accounts, disrupting financial transfers, and compromising communications where possible" (Ashok, 2016).

Support for unclassified cyber ranges emerged in tandem with the proliferation of cyber-attacks on government agencies as well as private sector organizations. In July 2013 Brigadier General Michael Stone from the Michigan National Guard announced his intention to launch one of the first unclassified cyber-exercise facilities in Michigan in accordance with this federal government priority. At a time when such facilities were rare and unclassified interstate efforts did not even exist, Stone cited key benefits of a nationwide network of cyber ranges, which included: 1) allowing "IT professionals without security clearance to practice for cyberattacks in multi-state and multi-stakeholder efforts," and, 2) to move beyond dependence on the federal government in the area of responding to and thwarting cyberattacks on state and local levels. He

added that, “85 percent of all people operating networks for critical infrastructure are civilians, non-federal government . . . and ultimately, it doesn’t make sense to put federal agencies in charge of critical infrastructure such as power grids and dams, because that’s not who’s operating them” (Wood, 2013).

Gaining support from public and private sector partners, mobilizing a cyber range network was intended to be an essential part of raising up a skilled workforce to address cyber security issues. “We have to do this,” Stone said (adding that it’s one thing to teach individuals to troubleshoot a network or solve a computer problem, but they need teams of people who can work together--collective training tools. “This is a clear trend. There’s a demand. Every time we ask a corporation if they want to participate, if they have any information assurance requirement, they get to ‘yes’ really fast” (Wood, 2013). Stone’s efforts spawned the Michigan Cyber Range (MCR), the largest unclassified cyber range in the country and home to MiC3 Cyber Civilian Corps in Michigan (Dunn, 2015), the leader among 50 states in digital first-responders—the state’s response force for security breaches, viruses and hacker attacks affecting state and local governments (Mulrine, 2015).

The perceived value of cyber ranges for effective cybersecurity training and the construction of cyber ranges around the country has since mushroomed. In August 2017 Maryland dedicated the first public cyber range facility in the U. S. in partnership with Cyberbit, an Israeli cybersecurity company whose "Range" platform was originally built for the Israeli Defense Force. The goal of the center is to help close the talent gap in the state’s cybersecurity industry where more than 12,000 IT and cybersecurity companies serve organizations like the National Security Agency and U.S. Cyber Command. Maryland is also home to 17 colleges designated National Academic Centers of Excellence in Cyber Defense.

One of the newest, Regent Cyber Range in the Institute for Cybersecurity at Regent University in Virginia, was announced in October 2017. Regent also leveraged Cyberbit’s cybersecurity training and simulation platform so that cyber “warriors in training” of diverse skill levels are able to practice strategies and gain experience against diverse assaults and breaches in a network architecture and traffic pattern context that simulates those they are tasked to defend, using tools like ones they would

have at hand in their real-life situation. The Regent Cyber Range platform also "offers numerous security tools and systems, including risk assessment tools, monitoring systems, security information and event management systems, forensic tools and supporting databases, as well as other network, security and cyber components" (Cyberbit, 2017) to enhance its value as a training and equipping resource.

Beyond Simulation and Audits: The Cyber Range

There is a point when the limitations of simulation software fail to adequately simulate real-world scenarios and the increasingly complex vulnerabilities that cyber warriors must face. Consequently, cyber range training is proliferating in government, business and public sectors, where defense agencies, enterprises and service providers are building or accessing cyber ranges that can equip personnel and also help them detect vulnerabilities and increase security protections for infrastructure and applications. The rationale that drives the cyber range concept includes, the need for cybersecurity personnel to gain experience in hyper-realistic simulations to effectively combat a variety of attacks and apply solutions to multi-dimensional IT security challenges. The growing volume and complexity of security tools and their specific integration to the entire cyber security architecture sets up what Cyberbit CEO Adi Dar (2016) calls "'security tools fatigue' -- the unmanageable number of tools, intelligence feeds and procedures in the security operation, which usually have significant amount of overlapping, need to be always updated and adapted to the ever-changing IT and cyber security architectures, and in many of the cases are not really contributing to the effectively of the security." This situation is compounded when the organization's security analysts are inexperienced, expected to configure and master this unmanageable number of security tools against an untried threat, possibly an advanced threat infiltration or takeover of an IT network, and also "understand the workflows and procedures, particularly within the context of their enterprise" that are impacted. These conditions set individuals and teams up for failure.

Cyber range benefits include, serving as 1) a test-bed for potential products, 2) a training environment with new products so that the security professional's skill set and performance improve significantly, 3) a team training environment to improve teamwork

dynamics and communication, and 4) a vehicle to simulate and train all company personnel on the breach playbook, on the business dilemmas that a breach raises, and the kinds and ramifications of possible decisions by company executives, e.g., to pay, negotiate or mitigate a ransom threat.

Dar (2016) predicts that,

". . . in the coming years cyber ranges and simulation-based training will become an inseparable part of IT security training, certification and ongoing qualification just as they have become so for air crew training. This approach will finally address the growing security tool fatigue as well as help security executives build a new generation of better cyber defenders.

Dar's sentiments have been echoed in various industry sectors. Rabon (2016) contends that modern security assessments have failed as a means to assess Information Technology/ Industrial Control Systems (IT/ICS), which are responsible for vital infrastructure resources. He asserts that the future of ICS cybersecurity is dependent upon using cyber ranges to make those assessments, and the sooner the better. Rabon (2016) reported that, Applied Control Systems figured that from the approximately "750 ICS hacks reported, the financial cost has been $30 billion, and in 2015 alone, ICS-CERT responded to 295 ICS incidents" across a range of industries. Citing key advantages cyber ranges offer over traditional security audits, which "indicate if a security mechanism is in place and configured to industry standards without specifying if the mechanism is effective." Essentially, a Security Technical Implementations Guide supplies standards for compliance, but "neglects to tell the tester if [implementation] improves the security posture of the system," and when auditors use the Assured Compliance Assessment Solution tool for testing security settings, there is no complementary method of testing the effectiveness of the settings in the working system. Most audits (e.g., DoD Information Assurance Certification and Accreditation Process-DIACAP and Risk Management Framework-RMF) also do not account for integration and traffic.

The dimension that cyber ranges offer analysts tasked with addressing these inadequacies is being able to "non-destructively" test the ICS thoroughly, without the down side of real-world impacts. The analyst could test devices beyond their prescribed

thresholds, assess the full range of their capabilities in an operating system where the repercussions of failure are not in play, and get an integrated assessment. Beyond security, Rabon (2016) and others see beneficial implications for engineers, "While engineers can plan and design for capacity, unless a system is operational the engineer cannot be sure the design has addressed the actual system bandwidth requirements. Cyber ranges would allow engineers to model and test systems using realistic traffic while identifying where potential issues may occur once the system is running," as well as address ICS issues related to OS updates, configuration changes and patching on a live critical industrial infrastructure system. Cyber ranges supply a uniquely valuable environment where developers can observe how patches, upgrades or reconfigurations actually affect the system's functioning capabilities before integration into the vital production system. Security devices, as well as new, untested hardware and software could be "test run" prior to adoption, to ensure nothing triggers damage or system shutdown. Unfortunately, often live systems are disrupted.

A recent example of such testing in the FCR [fault containment region] found an intrusion prevention device employed in a system model that could be made to fail open when subjected to the right kind of overloading. It would give up and pass all traffic through, good or bad (Winter, 2012).

This is something to find out in the cyber range setting, not in a real attack situation.

Cyber Range Optimization

In the industrial sector, the Honeywell cyber range provides an example of optimization. The process of optimization has five phases of customized development for the user; 1) Documentation and enumeration--approximating the actual user network and its traffic, 2) reconstruction of the target system environment through virtual machines, 3) verification via functional testing phase, 4) model the target system with traffic on the virtualized network, and, 5) final stage would include any or all of the following valuable exercises—red/blue exercises testing, hardware and software testing, modeling and simulation, independent validation and verification, research and development, tabletop exercises, comparative solution analyses, integration environment testing, patch testing, load testing, configuration testing, functional testing,

penetration testing, certification, training, hypotheses testing and team assessment (Rabon, 2016).

Multiple cyber range options are available, “as a service,” via public and/or private institutions, and other creative options. They vary in focus, scope, cost, and training. All, however, are designed to provide scalable, cost-effective platforms to recreate real-world threat scenarios that better equip personnel and enhance system-hardening purposes. Drawing on his expertise with adaptive computing platforms and quantum computing algorithms, Timothy Braje, (2016) a technical staff member in MIT’s Lincoln Laboratory Secure Resilient Systems and Technology Group, laid out key issues and goals for the optimization of cyber ranges for cyber defense. Cyber ranges are typically not connected to external networks (and thus have no access to the Internet or to network resources) as a preventive measure so that testing and training is not interfered with or networks damaged.

Braje expressed a growing need to quickly and accurately construct and configure networks, to describe the ranges/events that require execution, overlaying virtual users that automatically execute activities of real users in the context of the simulated network traffic generated, which are monitored via analysis infrastructure. Tools that optimize cyber ranges developed in the Lincoln Labs “extend automation capabilities, increase environment fidelity and scale” in size and complexity, including development of a standard event-description language, which enables the entire tool suite. Lincoln Adaptable Real-time Information Assurance Testbed (LARIAT) project leaders have actively worked with industry partners to develop a standard language that could be adopted by organizations in the cyber range business.

Other breakthroughs the team has made are in emulation—constructing an innovative traffic generator geared to real and specific user application interactions that exhibits distinct advantages over protocol emulation. Through information and resource sharing, LARIAT helps leverage defenders on to the playing field in both military and civilian sectors, well-equipped for the cyber defensive tasks confronting governments and business globally.

An alternative to constructing and deconstructing cyber ranges, are cyber ranges in a cloud sandbox. Quali, a leader in cyber sandboxes offers their clients access to

"self-service environments on-demand." According to Kiran (2017), the complexities of security testing for vulnerabilities, especially in large environments with many different infrastructure components-- servers, switches, firewalls and test tools, not to mention multiple APIs, GUIs and command line interfaces—makes "adopting a cloud sandbox orchestration platform [an optimal way to allow] teams to operate tools and practice cyber-defense postures without the added difficulty of learning to navigate various software interfaces, command syntaxes and GUIs." In addition,

A complete cyber range solution can also automate the deployment and configuration of all the necessary infrastructure pieces. Cloud sandboxes can replicate the elements for physical networking, storage, servers and test equipment, along with virtual resources, cloud components, tools and applications . . . users can even model and provision complex L1, L2 and L3 networking layers.

Sandbox users have the advantage of making rapid blueprint models. Kiran (2017) notes that this feature enables management of the "entire lifecycle of sandboxes with orchestration for automated setups, provisioning, monitoring, scaling and teardown." Snapshots can be captured and restored in the sandbox so that various threat situations may be re-enacted or rehearsed. The cyber range would also be valuable for performing "automated security regression tests, as well as streamlining live responses to exploits." Cyber range optimization should also include, "clear visualization and automation processes through a single pane of glass UI. This interface simplifies the user experience, providing graphical views across all cyber range environments."

Advanced Tools for Advanced Defense

On-demand cyber ranges like the Virtual Clone Network (VCN) offered by SimSpace (Ravello, 2015), can be accessed for free and fee-based professional IT, QA and security team training, as can The Cyber Range, available through Palo Alto Networks' partnership with Cyber Test Systems (Palo Alto Networks, 2017). These are affordable opportunities that would enhance an organization's IT capabilities, agility and network responsiveness.

Red Team-Blue Team type war games can also be run on cloud-based sandboxes. In fact, their environment is optimal for rapidly supplying full-stack, real-world cyberattacks because of tools that can model hardware and software, as well as

things like services, data, and applications in the context of the sandboxes. According to Kiran (2017), “This approach also allows for better posture management of legacy and often custom ‘made-to-order’ devices that are found in defense agencies.” Quali has enabled the Defense Information Systems Agency (DISA) to create efficiencies and cost reductions, consolidating its cyber range data centers on a private cloud. Ernest McCaleb, chief architect for DISA’s cyber security range said, “DISA is responsible for supporting a critical element of our national defense strategy, which is the sharing of information between joint war fighters, national leaders, and other mission and coalition partners; this fast, simple and cost-effective solution provides us with the ability to fulfill our mission without sacrificing performance or security” (Quali, 2017).

The Israeli Defense Forces (IDF) took the cloud sandbox to new levels in September 2017, paralleling real-time readiness training in the cybernetic area. In tandem with the Northern Command “Or HaDagan” exercise, a C4i and Cyber Defense Directorate official described the value of the cybernetic simulation, “In this exercise, for the first time, we’re fully testing and practicing on the cyber level. The Cyber Defense Division of the Directorate has been very dominant in its [IDF] operations.” (IDF, 2017). The big opportunity presented these cyber-commandos included testing some systems for the very first time, but more importantly, breaking new ground in an unprecedented way related to information and communication technology on the battlefield. “There’s a real challenge here to create a cloud network that travels with the forces,” says the military source. “Today, the entire IDF is connected to the network. There’s no ground unit and not a single platform that isn’t connected to the network, uniting the entire operation.” This cyber defense strategy, not only provides IDF connectedness, but serves to keep IDF networks safe from enemy infiltration. According to C4i and the Cyber Defense Directorate, “We want to confront the enemy before he can infiltrate the IDF network, and prevent him from getting in. Our goal is to catch him outside the network.” The IDF has also upgraded its bandwidth to be mobile, “We took capabilities that we had in the stationary world and copied them into the mobile world, maneuvering them in the field.”

The IDF is the vanguard for both cyber range optimization and advanced tools for advanced security defense. Essentially, their pioneering cybernetic drill moves the

concept of advanced tools for defense beyond the network into the realm of pre-emptive strikes outside the network, offering food for thought and support for the critical importance of hyper-realistic simulation training solutions. Another cyber defense vanguard, Massachusetts Institute of Technology Lincoln Laboratory LARIAT (Lincoln Adaptable Real-time Information Assurance Testbed) Range, has been a great asset to the U. S. Department of Defense and cyber range development. LARIAT's Project C has strategically created advantages related to Department of Defense cyber defense training with its capabilities of uniquely emulating every single government network and communication environment. Here is how it works. Project C sets cyber teams up so they work inside a "notional network-connected environment nearly identical to the real one they may be asked to defend"--ShoreNet for navy ships, missile defense command-and-control systems, power-grid-management networks or even field communications in battle. The results from participants in the Lab's Project C training often informs the trajectory of USCYBERCOM cyber defense training (MIT, 2016).

Conclusion and Future Study

As the cyber landscape continues to accommodate the malicious, vigilant and effective cybersecurity and the effort to equip cyber warriors will also continue to evolve. Cybersecurity Ventures predicts cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. Unlike other technology sectors that are driven by creating efficiencies and growing productivity, cybersecurity investments are an offensive strategy against cyber criminals. This may well turn into cybersecurity investments exceeding $1 trillion in the next five years (Morgan, 2016). Advanced tools for the increasingly advanced defensive measures required in this climate put cyber ranges, whether brick and mortar installations, cloud sandboxes, public or private, classified or unclassified, at the forefront of initiatives proving effective to raise up battle-ready cyber warriors and alliances committed to defense. It will be a daunting proposition, however, to fill the anticipated 3.5 million cybersecurity job openings by 2021 created by the need to deter cybercrime. This state of affairs elevates demand for and viability of cyber ranges of all kinds so that people can get effective training. It also elevates the benefits of resource-sharing and alliances--optimization of cyber ranges beyond the obvious. Alliances like the collaboration of Michigan Cyber Range with the

State of Georgia to set up their cyber range in Augusta (Corwin, 2017), a proposal for a federation of cyber ranges among EU and NATO nations (Vallaots, 2017), Ixia and Quali cyber sandbox collaborations with universities worldwide (Kiran, 2017), and, on a grassroots level, Palo Alto Networks' work with the Girl Scouts to offer merit badges in national cybersecurity (Lough, 2017).

Cyber ranges are an integral part in the growing demand for effective cybersecurity and for a paradigm shift in cybersecurity management "from the traditional, in-depth cybersecurity model, based on multiple layers of protection, to a new model . . . based on supercomputing and automation that mines and interprets data from previous threats to prevent future attacks" (Zakhour, 2016). This kind of "prescriptive security" could be formulated, tested and optimized in the cyber range environment--conceivably freeing up an organization's security personnel from threat detection, to applying "data analytics across complex, global IT architectures to detect, isolate and solve threats in real time." Cyber range optimization provides an essential resource for this challenge.

References

Ashok, I. (2016, June 20). The anatomy of a 'Cyber Jihad.' Retrieved November 12, 2017, from http://www.ibtimes.co.uk/anatomy-cyber-jihad-analysing-evolution-future-terrorism-cyberspace-1566184

BBC. (2011, June 17). US builds net for cyber war games. Retrieved November 30, 2017, from https://www.bbc.com/news/technology-13807815

Braje, T. M. (2016). Advanced tools for cyber ranges. Retrieved October 28, 2017, from https://ll.mit.edu/publications/journal/pdf/vol22_no1/22_1_2_Braje.pdf

Corwin, T. (2017, Apr 04). Georgia's $50 Million cybersecurity center to feature collaborative cyber range. Retrieved December 5, 2017, from http://www.govtech.com/security/Georgias-50-Million-Cybersecurity-Center-to-Feature-Collaborative-Cyber-Range.html

Cyberbit. (2017, Oct 03). Regent University and Cyberbit Open Cutting-Edge Cyber Range Training Center. Retrieved November 24, 2017, from

https://www.cyberbit.com/company/news/regent-university-cyberbit-open-cutting-edge-cyber-range-training-center/

Dar, A. (2016, Sep 21). The Cyber Range – Addressing the "Security Tools Fatigue." Retrieved November 12, 2017, from https://www.cyberbit.com/cyber-range-addressing-security-tools-fatigue/

Dunn, P. (2015, Dec. 16). Michigan Cyber Range. Retrieved December 3, 2017, from http://www.secondwavemedia.com/concentrate/features/MichiganCyberRange0351.aspx

Eichensehr, M. (2017, Aug 03). Baltimore Cyber Range training facility opens at Power Plant Live. Retrieved December 3, 2017, from https://www.bizjournals.com/baltimore/news/2017/08/03/baltimore-cyber-range-training-facility-opens-at.html

IDF. (2017, Sep 12). Training on our newest front: the cyber world. Retrieved October 29, 2017, from https://www.idfblog.com/2017/09/12/training-cyber-communications-defense-exercise/

Ixia. (2014). Cyber Range: Improving Network Defense and Security Readiness. Retrieved December 5, 2017, from https://www.testforce.com/testforce_files/newsletter/Aug_2016/ixia.pdf

Kiran, S. (2017, June 06). Orchestrating cyber ranges: A proactive approach to cyber security. Retrieved December 3, 2017, from https://techspective.net/2017/06/06/orchestrating-cyber-ranges-proactive-approach-cyber-security/

Lough, A. (2017, June 17). Ignite 2017: A Little More Action, Including Cyber Range! Retrieved December 5, 2017, from https://researchcenter.paloaltonetworks.com/2017/06/ignite-2017-little-action-including-cyber-range/

Morgan, S. Ed. (2017, Aug 29). Cybersecurity Ventures 2016 Cybercrime Report – hackerpocalypse: A cybercrime revelation. Retrieved November 30, 2017, from http://www.cyberdefensemagazine.com/cybersecurity-ventures-2016-cybercrime-report-hackerpocalypse-a-cybercrime-revelation/

Mulrine, A. (2015, Aug 17). Michigan's battalion of digital defenders raises bar for states' cybersecurity. Retrieved December 3, 2017, from https://www.csmonitor.com/World/Passcode/2015/0817/Michigan-s-battalion-of-digital-defenders-raises-bar-for-states-cybersecurity

Palo Alto Networks. (2017). Cyber range brief. Retrieved December 4, 2017, from https://www.paloaltonetworks.com/resources/techbriefs/cyber-range

Quali. (2017). Cloud sandbox for cyber range training. Retrieved December 4, 2017, from https://www.quali.com/solutions/sandbox-for-cyber-range-orchestration/

Rabon, C. B. (2016, July 20). Honeywell - securing our future: Why today's solutions cannot solve tomorrow's problems. Retrieved December 2, 2017, from https://www.slideshare.net/bsurfkid21/cyberrangewhitepapercbr070716finaldraft

Ravello. (2015, Aug 27). On-demand cyber ranges on AWS using Ravello - making cybersecurity development, testing and training affordable & accessible for enterprises. Retrieved December 4, 2017, from https://blogs.oracle.com/ravello/ravello-simspace-cyber-range-aws

Saadawi, T. & Jordan, L. (Eds.). (2011, May). Cyber infrastructure protection - Homeland Security digital library. Retrieved December 1, 2017, from https://www.hsdl.org/?view&did=5731

Winter, H. (2012). System security assessment using a cyber range. Retrieved December 3, 2017, from https://www.slideshare.net/bsurfkid21/cyberrangewhitepapercbr070716finaldraft

Zakhour, Z. (2017, Sep 07). The journey to self-learning cybersecurity. Retrieved November 30, 2017, from https://inform.tmforum.org/features-and-analysis/2017/09/journey-self-learningcybersecurity/?_ga=2.160855742.2038608747.1512072327-_1923528302.1512072327