FEATURES AND ARCHITECTURE OF THE MODERN CYBER RANGE: A QUALITATIVE ANALYSIS AND SURVEY

by

Ishaani Priyadarshini

A thesis submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Master of Science in Cybersecurity

Spring 2018

FEATURES AND ARCHITECTURE OF THE MODERN CYBER RANGE: A QUALITATIVE ANALYSIS AND SURVEY

by

Ishaani Priyadarshini

Approved: _____
Chase Cotton, Ph.D.
Professor in charge of thesis on behalf of the Advisory Committee

Approved: _____
Kenneth E. Barner, Ph.D.
Chair of the Department of Electrical and Computer Engineering

Approved: _____
Babatunde A. Ogunnaike, Ph.D.
Dean of the College of Engineering

Approved: _____
Ann L. Ardis, Ph.D.
Senior Vice Provost for Graduate and Professional Education

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my mentor, philosopher and guide Dr. Chase Cotton, who has extended his continuous support for my study and research. I thank him for his patience, motivation, supervision, knowledge and enthusiasm. His guidance has been a driving force not only for research, but also beyond that. As a research guide, he was ever assisting and would always improvise research tasks. He would provide ample opportunities and illustrious research ideas and allow me to choose whatever ideas caught my attention. As an advisor, he was always keen on assisting me with the courses that would prove to be beneficial for me. My knowledge base concerning cybersecurity has been broadened significantly over the last two years. I could not have imagined having a better advisor and mentor for my study. Without his supervision, I would have not been where I am today.

I would also like to thank the University of Delaware for giving me the platform and opportunity to accomplish the study.

I extend my vote of thanks to my family and friends who have also been very supportive. Their encouragement has been really valuable.

I also appreciate the valuable inputs from my colleagues Teddy Katayama and Fatema Bannat Wala who are not only graduate students at the University but are also researchers of Dr. Cotton.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Cybersecurity is one of the prominent global challenges due to significant increase in the number of cyber-attacks over the last few decades. To protect enterprises, personal data, productivity and to ensure a safe environment for work, cybersecurity awareness is very important. To prevent cyber infection, ad wares and to provide a consolidated solution, cybersecurity training is vital. Cybersecurity awareness and cyber security training are promoted by hyper-realistic virtual environments termed as cyber ranges. This study highlights the concept of cyber ranges, mainly in two sections. In the first section, several cyber ranges have been taken into consideration to identify significant attributes and classification based on several properties. An Ideal Cyber Range has been proposed taking into account the important parameters a cyber range should incorporate. In the second section, the Cyber Range at the University of Delaware has been introduced along with its fundamental working. The extensive study takes into account the components, scenarios and capabilities of the newly found cyber range. Finally, a comparison has been carried out between the already proposed Ideal Cyber Range and the Cyber Range at the University of Delaware to comprehend the proximity between the two. This would be of great assistance in future for determining the strength and weaknesses of the Cyber Range at University of Delaware considering what the range

is capable of at present and what could be done in future for the Range to become Ideal. We rely on different graphs to bring out the variation between the Ideal Cyber Range and The Cyber Range at the University of Delaware on basis of certain parameters.

Chapter 1

OVERVIEW

As we know, cybersecurity is one of the biggest concerns in today's world. The reasons could be many ranging from outdated software to default passwords that lead to cybercrimes. While technology flourishes, cybercrimes get more sophisticated. In a world where cyberspace is regarded as the fifth domain of war, it is necessary to be prepared against the crimes by appropriate cyber security training. Cyber ranges fulfill those purposes. As concerns related to cyber security grow rampantly, more and more cyber ranges are being deployed by the government, commercial organizations and research centers. According to the National Institute of Standards and Technology (NIST), cyber ranges are defined as interactive and simulated representations pertaining to an organization's local network, system, tools, and applications. Cyber ranges allot a safe and legal environment for users to gain hands-on experience to develop cyber skills and train themselves for creating a secure environment [1]. Cyber ranges can work either individually or operate with other cyber ranges. They may be stationed by governments, industries and academic institutions. They rely on hardware and software or a combination of both along with network components and support certain network services. Cyber ranges are crucial simulation environments for people who need hands on experiences and to test new ideas to solve complex cyber problems. They can be used to assess performances and ensure real time feedback.

Since the environment is setup for warfare training several teams can participate to improve teamwork and team capabilities. The teams can identify and mitigate threats using real world tools in the given environment. Hence cyber ranges prove to be beneficial for information technology professionals, organizations, students and academic researchers.

Cyber-attacks are on rise these days, thus making cyberattack epidemic just round the corner. The attacks could range from something very trivial like eavesdropping to something highly significant like the Denial of Service attacks. The remarkable compensation caused in form of loss of property or finance demands immunity against such insecurities. A cyber range which may also be thought of as a virtual environment or a simulation platform which aids in delivering security professionals with certain skills and insights to thwart cyber-attacks. A cyber range ensures that professionals work together as a team across several security domains in order to improve their ability and defend against several attacks. The behavior of certain attacks from several network capabilities may be studied in a cyber range. Deploying cyber ranges minimizes the cost of simulating security testing. A combination of automation may be useful in increasing agility and responsiveness. As cyber ranges are controlled virtual environments, certain performance results may be duplicated to prevent further failures and errors. A Cyber-Range capability offers a practical and controlled setting where attack scenarios and security responses can be evaluated in real-world conditions and recorded and analyzed to improve the overall resilience of

target networks [2]. The idea is to potentially harm an organization's network in order to understand how to protect it. A cyber range incorporates certain teams, each depicting their own influence. As many as seven teams have been talked about so far. They are as follows.

- Red Team
- Green Team
- Blue team
- White Team,
- Yellow Team
- Grey Team
- Purple Team

The Red Team is responsible for attacking users' computers using certain vectors of infection such as virus, Trojans, malwares etc. whereas the Blue Team manages the availability, scalability, security and stability of network infrastructure and application infrastructure. The Green Team is responsible for simulating legitimate users over wire or wireless connections with their desktops, laptops, tablets, smartphones to the application infrastructure hosted on the network infrastructure managed by Blue Team. The Yellow team reports situational awareness whereas the White Team creates the cyber-attacks scenarios in order to monitor success or failure of blue team to defend properly against cyber-attacks which have been previously launched by red team. The Grey team represents normal traffic and service requests that must be maintained. While monitoring the same the White Team takes into account

availability, scalability, security and performance of network infrastructure and application infrastructure for Green team. In rare environments one can find a Yellow team which replicates innocent users clicking on a phishing link or innocently installing malicious applications, compromising the network's security. Finally, the Purple team, is a collaboration of a red team and a blue team i.e. both offensive and defensive techniques. The offensive method deals with tactics, techniques and procedures while, the defensive method deals with improving detection and response capabilities.

Being virtual environments they are not only restricted to an organization's local network but also range from single standalone ranges in an organization to internet replicating ranges which could be accessed from around the world such that they can be used by private as well as public organizations along with students, researchers, trainers and education providers [1]. Based on their purpose of utilization, cyber ranges may be classified as follows [3]

- **Military, Defense and Intelligence**- Military organizations and government agencies require cyber warriors with befitting skills to counter cyber terrorism. Weaknesses and vulnerabilities are critical to the nation's infrastructure. Hence the Military and Defense implement large scale cyber ranges like Defense Advanced Research Projects Agency (DARPA)'s National Cyber Range (NCR). DARPA's primary aim is to replicate large networks for Department of

Defense (DOD) weapon systems and operations. A realistic testing facility is provided for research. Apart from enabling the development and deployment of state-of-art cyber testing capabilities, it could also facilitate scientific use of cyber testing methods. DARPA also sees to it that a virtual environment is provided for qualitative, quantitative and realistic assessment of cyber technologies for research and development. U.S. Army Communications-Electronics Command, or CECOM,has proposed a cyber range that is capable of developing configurations for supporting multiple environments through the cyber range. It has also been observed to incorporate features like Cyber Threat characterization and dynamic threat capability [4].

- **Education**- The idea of 'Cyber Range for education' came up in 2015. The idea was to provide training on cyber-attack, defense and detection, for developing certifications, to collaborate with industries, carry out researches, and to offer training for military and veterans. The Virginia Cyber Range offers cyber range for Education. Certain Cloud based cyber ranges boost the number of trained cyber professionals. The Michigan Cyber Range encourages teaching, testing and training. Apart from being digital playgrounds, these cyber ranges offer a repository of course materials that the educators and students can benefit from. These ranges offer defensive trainings primarily such that students can imitate to be network administrators and study simulated attacks.

- **Enterprise and Commercial**- A cyber defense center is effective if people can operate it and defend enterprises. Enterprises and commercial organizations deploy cyber ranges to conduct games and simulations in order to strengthen cyber security capabilities. These commercial organizations need a superior way to develop ranges so that they are at par with the rapid growing applications, threats and traffic volumes. They provide cyber range solutions to create an operationally relevant environment that mirrors Global Information Grid (GIG) and enables sophisticated simulations and manage a distributed network of cyber ranges. The Pinecone Cyber range is one such Commercial Cyber range. The IBM X Force Command Centre is the first ever commercial cyber simulator and uses live malware to test security.
- **Service Providers** - The Cyberbit cyber range is one of the world's leading provider of cybersecurity training. It creates new business lines by setting up cybersecurity training and simulation centers and ensuring advanced training and testing services [5].
- **Open Source**- Security professionals need practical real world experience. However, performing dangerous activities on production, personal or work networks may lead to serious consequences. The Arizona Cyber Warfare Range is a safe environment for learning, hacking, testing, war games, malware practices and real opponent challenges. The range also provides free, internet accessible and safe environment for novices and experts to test their skills and conduct security practices.

- **Law Enforcement**- According to Computer Security Institute (CSI)'s survey, thirty four percent of respondents reported intrusions to law enforcement [6]. Applications in military and law enforcement are being developed and tested in cyber ranges. This determines their feasibility and effectiveness in practice. The Michigan Cyber Range is one such cyber range. A cyber range environment makes use of a lot of computing devices and every device used increases the vulnerability of a cybercrime. Law enforcement can respond to the resulting cybercrimes. They also ensure technical help with forensics and investigation along with training, victim services and community education [7].
- **Others**- Apart from being useful for the domains discussed above, cyber ranges may also offer miscellaneous assistances to Incident Handlers and for Continuity of Operations. As common attack techniques could be analyzed, one can respond to attacks when they occur. Malicious applications and network activity could be monitored. Network vulnerabilities and root causes of incidents become easy to identify as the configuration of cyber ranges can lead to incident response. IBM X-Force Command Centre is one such cyber range. Security incidents can lead to disruption of continuity of operations. Often cyber ranges provide redundant and resilient systems for supplying functions in such scenarios.

In the succeeding section we will take a look at the cyber ranges taken into consideration for the survey process. Corresponding to the thesis, which takes into account two sections, we present the survey in two parts respectively.

Chapter 2

RELATED WORK: A SURVEY ON THE EXISTING RANGES

This thesis highlights two sections. The first section deals with the general survey of few cyber ranges with the aim to extract significant parameters on basis of which we propose an ideal cyber range. The second section focuses primarily on the Cyber Range at the University of Delaware, which is affiliated to the University. The corresponding survey highlights some cyber ranges which are affiliated to their respective universities.

The survey for the former section is as follows.

According to NIST, Cyber ranges can be termed as responsive simulated depiction of an institution's local network, system, tools, and applications that are connected to a simulated network environment [1]. They ensure safety and provide a legal environment to implement cyber security skills and security testing. It could incorporate hardware, software, virtual machines and the internet could encompass simulated traffic, webpages, browsers etc. The concept of cyber ranges is not very old. It is still evolving. As cyber ranges surround multiple features and functions, the analysis is limitless. In this section we come up with a few related work on cyber ranges. Further we have contemplated several cyber ranges as a part of the related work, to analyze them, and familiarize ourselves with their assets and limitations. The

analysis will not only acquaint us with parameters that aid in functioning of a cyber range but will also be useful in proposing an ideal cyber range.

Davis [3], proposed a survey on cyber ranges and the respective testbeds. The researchers have classified the ranges into military and government, academic, commercial and modelling and simulation based. Apart from highlighting several cyber ranges already published, they also provide information on whether the ranges are simulation driven or emulation driven. For emulation driven cyber ranges they have used testbeds with real hardware or software. Emulation Cyber ranges are capable of creating environment for training and testing and to perform high fidelity and repeatable experiments. The only limitation it seems to have is a complicated infrastructure which leads to an increase in the cost. Virtualization or resource sharing could provide some aid in this situation. For simulation based cyber ranges, software models of real world objects are used. This makes simulation scalable and flexible. The foremost issue a simulation driven cyber range deals with is that it is difficult to verify whether it is feasible or not, thus making emulation driven cyber ranges more preferable.

2.1 Survey 1

. The following Cyber Ranges have been analyzed for the research.

2.1.1 National Cyber Range (DARPA)

National Cyber Range is a cyber range created by the Defense Advanced Research Projects Agency (DARPA) to provide national level virtual facility for testing software and running network simulations. The range supports an open architecture design and can be configured as required by different events. The capabilities range from traffic generation, thread injection, patch levels and network services to testing, evaluation, interoperability assessment of devices and applications. It uses tools like the Systems Administrator Simulation Trainer (SAST) and Breaking Point. SAST provides realistic cyber range environment for training, testing and conducting exercises. The software incorporates a suite of tools, known as A Network Traffic Synthesizer (ANTS). A multi user traffic tool can track network traffic. Breakpoint can model real world applications, live security attacks and users. It can also perform network management, script test data and emulate networking protocols. Apart from the sophisticated tools and reliable architecture, the cyber range is known for public key interface, control access cards, classified environment, wireless capabilities and Voice over Internet Protocol (VoIP).

2.1.2 Michigan Cyber Range

The Michigan Cyber range was launched to assist cybersecurity professionals deal with real world implications. It provides a secure environment for training, testing and education. It is also a forum for research and industrial control systems security. It is run by trusted network provider Merit. The cyber range relies on Merit for conducting

cyber security certification courses, training exercise and operating Sandbox services which are quite flexible. It ensures that the cyber range is accessible worldwide. The Secure Sandbox is located in the virtual cloud and simulates real world network environment with virtual machines that act as several servers and machines. The other fields that the cyber range will take into account are infrastructure defense, homeland security, criminal justice and law enforcement, academics and businesses. The following depicts Michigan Cyber Range [15].

Figure 2.1: Michigan Cyber Range

2.1.3 Virginia Cyber Range

The Virginia Cyber Range was designed to promote education in cybersecurity. The isolated servers and dummy machines in the range are vandalized deliberately for educational purpose. It is a defense training center that encourages analysis of simulated attacks and also provides hands on exercise to students through their web

browsers. It is a cloud hosted virtual environment, the cloud services being Amazon Web services. The range is already serving around 250 students and hopes to expand the number of students to 2500 [4]. The resources are provided at no cost to students. The tools supported for this cyber range are mainly for students, so they are available online and are mostly free. The following depicts Virginia Cyber Range [16].

Figure 2.2: Virginia Cyber Range

2.1.4 IBM Cyber range

IBM's X-Force command centers are the first physical cyber range for the commercial sector with an aim to help clients respond to cybersecurity incidents. It focuses on how companies can deal with massive data breaches after they occur and also how to prevent them. The cyber range boasts of Resilient Systems' Incident Response platform, which supports one of the largest privacy databases and can span the entire lifecycle of an attack from detection to response QRadar Security Intelligence

Forensics that can be instrumental in log management, anomaly detection and vulnerability detection. The setup can incorporate thirty six operators [5]. The security operations are staffed by fourteen hundred professionals [6], and uses live malware, ransomware and real world hacking tools from dark web to delve into the cyber security world. The clients can test their environments, run attack scenarios and identify critical processes to chalk out responses. The following depicts IBM Cyber Range [17].

Figure 2.3: IBM Cyber Range

2.1.5 CRATE

The Cyber Range and Training Environment (CRATE) is developed and maintained by the Swedish Defense Research Agency to deploy and configure several virtual

machines in a supervised environment. It encompasses host based traffic generators emulating user behavior and tools for observing the environment. The physical infrastructure has around 800 servers. The network infrastructure can be configured as needed and a large number of operating systems and applications can be deployed. CRATE has been known for its vulnerability assessment and intrusion detection [7]. It uses visual and textual tools for intrusion detection, simulation tools and security management tools for cybersecurity training. CRATE applications are compatible with both Linux and Windows machines. A graph based user interface can allow manipulation of parameters that control the operating system, firewall, application, software, network topology and users. The following depicts CRATE [18].

Figure 2.4: Cyber Range and Training Environment (CRATE)

2.1.6 Cisco Cyber Range

The cyber range developed by Cisco uses real world conditions in a synthetic war gaming environment to help staff build skills and experience to combat cyber incidents. It uses advanced tools and techniques to mitigate cyber-attacks. The cyber range has four components: operations based models to respond to threat scenarios, platform based security tools, simulations for real applications, continuous updating and upgradation and a cloud hosted environment [8]. The infrastructure supports wired, wireless and remote access along with client simulator, server simulator and application simulator [9]. The cyber range utilizes five hundred malware samples, ransomware and attack cases to deal with the realistic cyber-attack scenarios. The comprehensive integrated services offered by the Cisco cyber range include cyber range workshops that give individuals experience regarding real life cyber-attacks and defenses, cyber range subscriptions which offer threat reports so that latest threats can be monitored and assistance in re-creating similar labs. The following depicts Cisco Cyber Range Workshop [19] and Cisco Cyber Range [20].

Figure 2.5: Cisco Cyber Range Workshop

Figure 2.6: Cisco Cyber Range

2.1.7 Cyber Range at the University of Delaware

The Cyber Range at the University of Delaware is exclusive to students for developing and practicing skills in various scenarios to test programs for security flaws, build coding skills, respond to attacks and countermeasure techniques. With 24 seats and 6 individually controlled room monitors the cyber range is dedicated to generating, monitoring and capturing traffic. Individual and group exercises along with Capture The Flag (CTF) type events are conducted often. The cyber range is at a nascent stage and lacks a lot of features as compared to the other cyber ranges, however in the coming years the cyber range is likely to allow multi-facility activities and also support facilities like cloud infrastructure and virtual private networks. The following depicts Cyber Range at University of Delaware [21].

Figure 2.7: Cyber Range at the University of Delaware

2.1.8 NATO Cyber Range

The North Atlantic Treaty Organization (NATO) conducts cyber related, training, exercise and education in a secure environment. The annual cyber defense exercise is one of the two largest international cyber defense exercises, namely 'Cyber Coalition' and it helps cyber experts develop their capabilities through realistic challenges [10]. The cyber range can implement electronic warfare, test and rehearsal, mission refinement capabilities by using various tools, techniques and procedures and encouraging red and blue teams to participate in various cyber exercises. The following depicts NATO Cyber Range [22].

Figure 2.8: NATO Cyber Range

2.1.9 Department of Defense (DOD) Cyber Range

The DoD cyber range promises cyber security aid to several governmental operations pertaining to the army, navy, air force and several other organizations like Defense Information Systems Agency (DISA), National Security Agency (NSA) and Office of the Secretary of defense (OSD). It is capable of conducting penetration testing and incident responses and accessing certain cyber related techniques and tools. The focus is to provide cyber warriors an environment identical to the daily battle field of cyber incidents. It relies on traditional storage platform but is not very scalable [11]. As the environment is dynamic, the number of machines cannot be anticipated. The cloud platform associated is Tintri which also provides a modelling and simulation environment to the cyber range. The Cyber Range relies on Tintri for disaster recovery and for viewing multiple VMstore's in a single pane of glass thereby leading to a better performance evaluation.

2.1.10 Raytheon Cyber Range

Raytheon cyber range provides customized virtual environment to enhance cyber operations, training and assessment capabilities [12]. A broad range of tools and the capability to automate lead to its stability and performance. It can rapidly set up and tear down complex test environments. The architecture supports separation of test environments from range environments and functions. It encourages hardware in the loop testing capability so that real systems can interact with virtual environment and can capture any traffic in an event. The operating procedures can easily adapt to

customers' requirement. The architecture allows simulation of networks ranging from a single physical host to tens of thousands of virtual hosts running in a cloud computing environment. It is scalable, extensible, flexible and automated. The following depicts Raytheon Cyber Range [23].

Figure 2.9: Raytheon Cyber Range

2.1.11 Baltimore's Cyber Range

The Baltimore cyber range is available to both government and industry professionals. For cyber training and simulation it has collaborated with Cyberbit Inc. to provide a hyper realistic virtual environment for training and testing. It incorporates advanced Security Operations Centre (SOC) tools along with network tools and traffic generators for simulation, attack detection and compromise remediation. The range is known for replicating complex enterprise networks for training and targeting real

world attacks. The training manager can define, build, deploy and run training scenarios whereas the trainee activities are tracked and recorded with logs [13]. For training security professionals, the range relies on Supervisory Control And Data Acquisition SCADA and control systems hardware to simulate SCADA attacks. Attack familiarization, attack detection and compromise remediation are basic training given to students and professionals.

2.1.12 Florida Cyber Range

The Florida Cyber Range is co-operated by University of West Florida and a cybersecurity training and simulation leader Metova Cybercents. The range presents training and testing solutions for academic, government, military and industry organizations by introducing various cyber security related exercises, operations and research. The aim is to provide cybersecurity expertise to the nation [14]. The areas taken into consideration are penetration testing, ethical hacking and networks and systems security. Defensive cyberspace operations and cyber war games make it one of the most capable cyber ranges. It works in an integrated live virtual constructive cyber range environment for training and testing. The following depicts Florida Cyber Range [24].

Figure 2.10: Florida Cyber Range

2.2 Classification of Cyber Ranges

Based on the survey above, the cyber ranges can be classified on basis of a lot of factors. They are as follows

2.2.1 On basis of Infrastructure association (Public / Private / Federated)

The cyber ranges discussed above could be classified on basis of infrastructure association as Public, Private or Federated. We can group the cyber ranges into appropriate infrastructures. The federated infrastructure incorporates cyber ranges like NCR, CRATE, NATO, Raytheon and DoD whereas the IBM cyber range belongs to the private infrastructure. CISCO cyber range, Baltimore cyber range and Virginia cyber range belong to both public and private infrastructure groups. It has been observed that the Michigan Cyber range and

the Florida cyber Range belong to the all the classifications. The classification is depicted in the following illustration

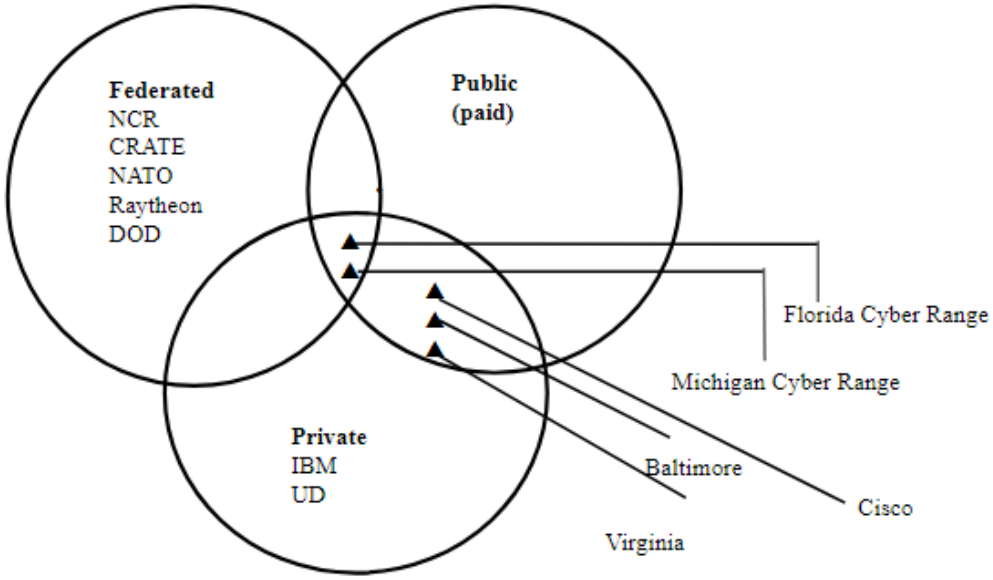


Figure 2.11: Classification of the cyber ranges as public, private and federated

2.2.2 On basis of whether a Cyber Range deploys cloud, Virtual Private Network or No Cloud

The cyber ranges considered above can be classified on basis of the fact if they use a cloud platform or not. Additionally, we have seen that some ranges deploy Virtual Private Network (VPN) and some rely on Virtual Clone Network (VCN). We observe that all cyber ranges that use the cloud platform, also deploy VPN except the Cyber Range at the University of Delaware which deploys a VPN but not the cloud infrastructure. While cyber ranges like

Virginia, IBM and Florida use cloud platform, others like Cisco, DOD, Michigan etc. support cloud as well as VPN. None of the above discussed cyber ranges can be classified in the third category of VCN, however ranges like Ravello implement VCN and UD cyber range may deploy it in future. The classification may be comprehended from the table given below.

Cloud Infrastructure (Only)	**Cloud Infrastructure and Virtual Private Network**	**No Cloud Infrastructure**
Virginia	Cisco	Cyber Range at UD
IBM	DOD	
Florida	NCR	
	Michigan	
	CRATE	
	NATO	
	Raytheon	
	Baltimore	

Table 2.1: Classification of cyber ranges on basis of whether they deploy cloud, cloud along with VPN, or no cloud

2.2.3 On basis of different teams they support (Red, Blue, Green, Yellow, Purple, White, Grey)

The cyber ranges can be classified into yet another type taking into account the teams they incorporate. Different cyber ranges are equipped with different group of people (students/ professionals/customers). They may support several different kinds of tools and platforms. Based on their operation environments and purpose they can host different kinds of teams. Red and Blue teams are common for all the cyber ranges. However some ranges like the NCR also support a grey team [8]. NATO supports as many as red, blue, yellow, white and green teams [9]. Some cyber ranges also encourage purple teams, like the Cyber Range at the University of Delaware. The table below shows how the ranges can be classified based on the teams they encompass. N (No) represents lack of the team whereas Y (Yes) represents presence of the team in the Cyber Range.

CR Teams	Red	Blue	Green	White	Purple	Yellow	Grey
NCR	Y	Y	N	N	N	N	Y
Michigan	Y	Y	N	N	N	N	N
Virginia	Y	Y	N	N	N	N	N
IBM	Y	Y	N	N	N	N	N
CRATE	Y	Y	N	N	N	N	N
Cisco	Y	Y	Y	N	N	N	N
UD	Y	Y	N	N	Y	N	N
NATO	Y	Y	Y	Y	N	Y	N
DOD	Y	Y	N	N	N	N	N
Raytheon	Y	Y	N	N	N	N	N
Baltimore	Y	Y	N	N	N	N	N
Florida	Y	Y	N	N	N	N	N

Table 2.2: Different teams supported by the Cyber Ranges

2.2.4 On basis of whether Cyber Ranges deploy Virtual Machines or Sandboxes

Yet another way of classifying cyber ranges is on basis of testing environments in form of virtual machines and sandboxes. Even though both are ways to provide isolation and may not be possessing the capability to avert malicious activities taking place within an application, they can be differentiated on certain grounds. Since they are implemented in different ways, they possess

different softwares, files and operating systems. While virtual machines are heavy and provide complete isolation, sandboxes are light weighted and provide flexible isolation. All the cyber ranges we have taken into consideration deploy virtual machines and some of them consider sandboxes as well. The reason why cyber ranges do not solely rely on sandboxes is because testing of malwares inside virtual machines is safer than testing it in sandboxes. As sandboxes provide flexible isolation, they are insufficient for testing sophisticated malwares and malware may affect the periphery. However since virtual machines provide complete isolation, there is limited contact to applications, browsers and storages. We have classified the cyber ranges on basis of whether they support virtual machines solely or rely on both virtual machines and sandboxes. The classification is as follows. Y (Yes) represents presence whereas N (No) depicts absence.

Cyber Range	Virtual Machines Only	Virtual Machines and Sandbox
NCR	Y	N
Michigan	Y	Y
Virginia	Y	N
IBM	Y	Y
CRATE	Y	N
Cisco	Y	N
UD	Y	N
NATO	Y	Y
DOD	Y	Y
Raytheon	Y	Y
Baltimore	Y	N
Florida	Y	N

Table 2.3: Virtual Machines and Sandboxes deployed by Cyber Ranges

2.3 Survey 2

Likewise, the survey for the latter section is as follows.

As we know cyber ranges are deployed by several organizations belonging to the government, military and academics. The cyber range at University of Delaware is a forum for students and researchers to gain expertise in cybersecurity training. In the

past, several universities and academic institutions have come up with the idea of establishing cyber ranges for their students are researchers. In this section, we will take a look at a few of them.

2.3.1 Regent Cyber Range

The Regent Cyber range was launched on Oct 3, 2017 in partnership with Cyberbit. Ltd. The cyber range aims to provide hands on experiences, training and simulation platforms with real time attack scenarios and security breaches. The cyber range is not only limited to students and researchers but is also a learning center for the government, military and business organizations. It is fully customizable and provides full virtualization in order to meet specific training requirements. Moreover, it is capable of identifying threats and vulnerabilities so that users may develop countermeasures and updated protocols so as to deal with critical attacks. Various network tools and systems such as the risk assessment tools, monitoring systems, security information and event management systems, forensic tools etc. are made available for the training process. The cyber range also hosts meetings with industry and government leaders to highlight cyber security related topics. The following depicts Regent Cyber Range [25].

Figure 2.12: Regent Cyber Range

2.3.2 Virginia Cyber Range

The Virginia Cyber range became functional in September 2016. The virtual center can accommodate two hundred fifty students and is capable of offering isolated servers and dummy machines. It is expected to accommodate up to twenty five hundred students in near future. It is powered by Amazon Web Services and provides defensive training so as to make students and researchers adept in cyber security training. It is a public and private sector collaboration also encourages other universities like George Mason University, James Madison University and Northern Virginia Community College to explore the cyber range. The cloud based environment strengthens deployment and scalability. It also arranges exercises and capture the flag (CTF) events.

2.3.3 Florida Cyber Range

The University of West Florida Centre teamed up with Metova Cyber CENTS to come up with the Florida Cyber Range later in 2017. The cyber range is an online environment that encompasses virtual platforms, hands on practice, operations, training and research, which proves to be beneficial for the government, military and industrial organizations. It also focuses on cybersecurity education, exercises, competitions and conferences. In the cybersecurity training operations, the most popular ones are penetration testing, network security, defensive mechanisms and ethical hacking.

2.3.4 Wayne State Cyber Range

The Wayne State University has come up with a cyber range 'Cyber Range Hub' for students and professionals seeking cybersecurity understanding. The hub will also be looked after by the Merit Network, the Advance Michigan Defense Collaborative and the Michigan Economic Development Corporation. Several workshops pertaining to ethical hacking, digital forensics, penetration testing and Capture the Flag events are organized. It also features secure sandboxes for testing systems and applications. The following depicts Wayne State Cyber Range [26].

Figure 2.13: Wayne State Cyber Range

2.3.5 Arkansas Cyber Range

University of Central Arkansas acquired a half million dollar grant from the Arkansas Department of Higher Education to invest in building a cyber range that would cater to the educational development of students in cyber security. It is confined to the University of Central Arkansas and it allows professors to create networks so that students can anticipate the different cyber-attacks that are prevalent and the appropriate technology to perform cyber defenses. The range also boasts of setting up any kind of network that would experience injecting of certain viruses to analyze them and defend systems against their infections, without actually having the viruses spread through the internet. The focus of the range is to train students so that they can establish cyber security in real time systems. The following depicts Arkansas Cyber Range [27].

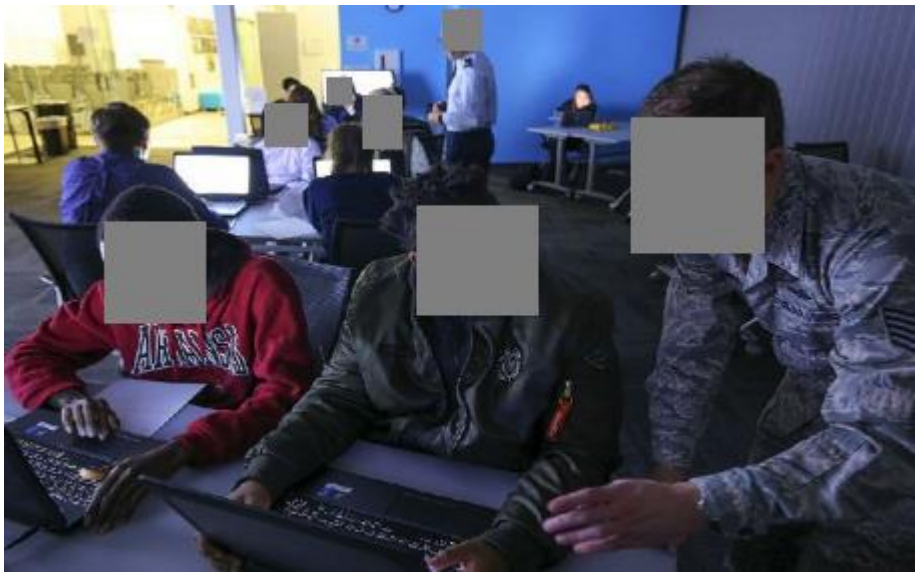


Figure 2.14: Arkansas Cyber Range

2.3.6 Michigan Cyber Range

The Michigan Cyber Range is a step ahead of most of the cyber ranges affiliated to the Universities in sense that it provides industry recognized certifications along with cybersecurity training. Established in 2012 and powered by the Merit Network, the range offers educational institution to students, workforce to technology professionals and as a manufacturing base to the federal organization and security industry. It provides platform for conducting cybersecurity exercises and attack simulation. It has its own Secure Sandbox Service that encourages cybersecurity activities and software testing.

2.3.7 Georgia Cyber Range

The Georgia Cyber Innovation and Training Center is a rage at the Augusta University Campus. The state owned facility encourages modernized cybersecurity training for both public and private organizations. The cyber range also ensures cybersecurity protection by providing solutions to cyber related emergencies. Collaborating with private industries lead to economic development, whereas collaborating with inter-agency collaborations lead to efficient services. It also provides a cost effective platform for carrying out cybersecurity training. The unique feature offered by the cyber range is introduction of a Sensitive Compartmented Information Facility (SCIF) that allows training of sensitive information without affecting the other assets [14]. The following depicts Georgia Cyber Range [28]

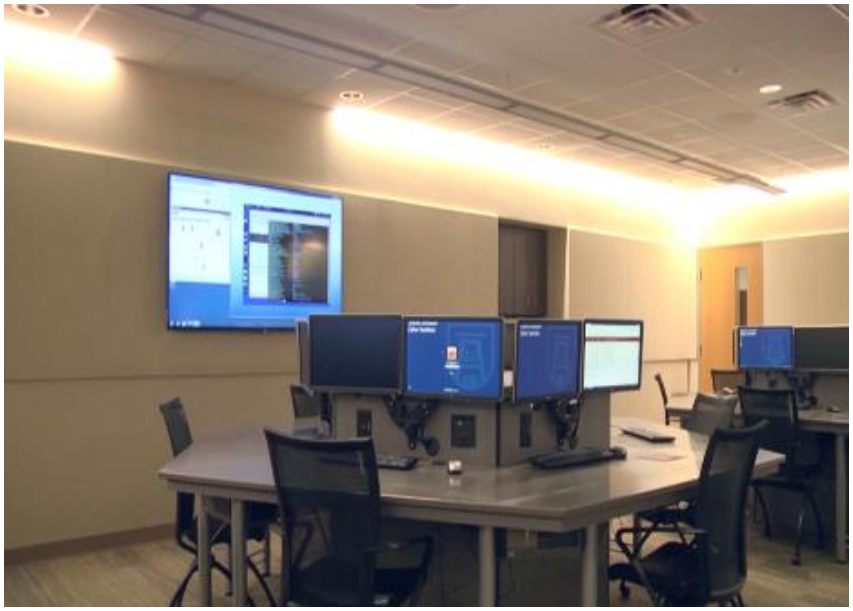


Figure 2.15: Georgia Cyber Range

2.3.8 Arizona Cyber range

The Arizona Cyber Warfare Range (AZCWR) has been hosted by the Grand Canyon University for cybersecurity training. The live-fire cyber warfare is equipped with laptops, servers and other equipments in the 4500 square foot zone and is accessible to everyone. The cyber range provides assorted hands on practice on cybersecurity exercises like password cracking, system break ins, system hardening etc. it is dedicated towards expanding the cybersecurity landscape so as to increase cybersecurity warriors in future. The following depicts Arizona Cyber Range [29].

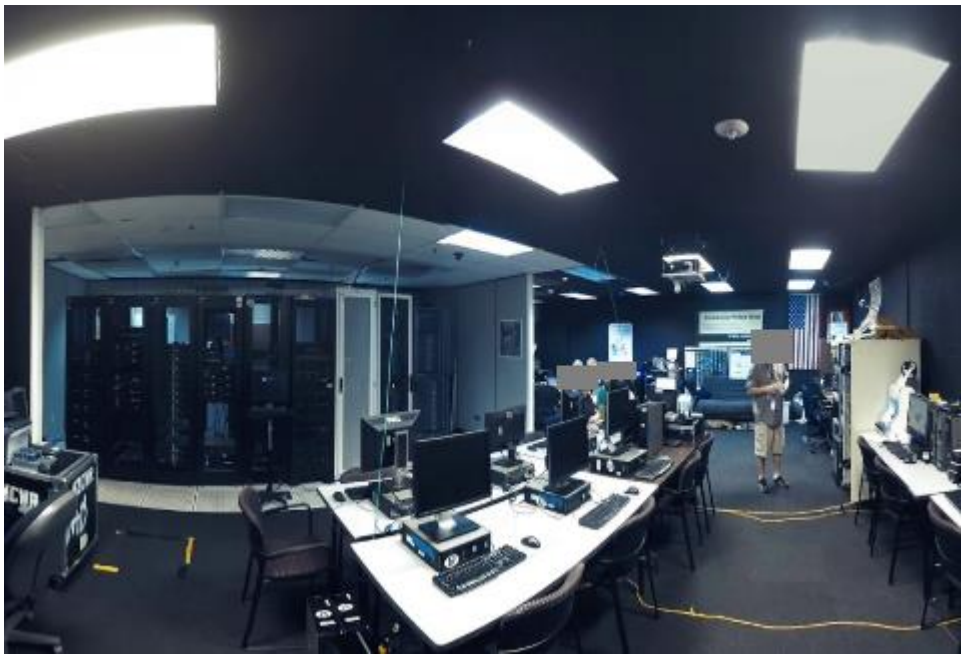


Figure 2.16: Arizona Cyber Range

In this section, we have considered the cyber ranges that already exist. Based on the survey, we have analyzed the ranges and classified them on basis of certain features. Several tables have been used as a means to represent classifications. In the succeeding chapter, we will be introducing the Ideal Cyber Range based on certain significant parameters that cyber ranges should incorporate.

Chapter 3

INTRODUCING THE IDEAL CYBER RANGE

In this chapter, we will list down a few parameters that are essential for cyber ranges. Based on their significance to the cyber ranges, we will assign them qualitative values. These qualitative values will assist in proposing the ideal cyber range.

3.1 Essential Parameters in Cyber Ranges

Since cyber ranges are operation oriented, their performance depends on certain parameters. These could range from number of seats to infrastructure, creating some sort of impact on the functioning of ranges. We have discovered few such parameters in this section. Based on the gravity of functions, and significance of these parameters we have assigned them some unquantified values i.e. very low, low, medium, high, very high. These values provide aid in proposing an ideal cyber range and plotting graph for the same. The parameters are as follows.

- **Seats**- The size of cyber ranges may be defined by the number of seats and the systems encompassed. While cyber ranges like UD cyber range are limited to twenty four seats, there are cyber ranges that have a seating of three hundred twenty like the Georgia Cyber Range [14]. Certain operations would require users to be a part of the cyber range while performing the operations as many

sophisticated platforms and machines are limited to the cyber range and may not be available to remote users. However for carrying out exercises and Capture The Flag (CTF) like competitions which do not use tools and systems specific to the cyber range, students can participate remotely and seating is not a big concern. Students, researchers and professionals are encouraged to bring their own machines keeping in mind the different tools that are confined to different operating systems. However, since cyber ranges incorporate functions that are exclusive to the ranges, the parameter requirement could be Medium.

- **Infrastructure** - Cyber ranges is have specific infrastructure owing to their functions. Since different cyber ranges have different capabilities, they are equipped with disparate infrastructures. The Raytheon Cyber range has an agile range architecture to enable emulation multiple host platforms. The architecture allows separation of test environments and enables hardware in loop testing capabilities. More than forty Standard Operating Procedures are responsible for simulation, mission services and future connectivity. The National Cyber Range NCR has infrastructure, instruments and workforce that could be integrated into a simulation environment. It supports an infrastructure that is a combination of several infrastructures and architectures. The Department of Defense (DoD) network infrastructure is complicated with many layers of security. The layers boast of vulnerability scanning, antivirus protection, website and email filters along with Intrusion detection Systems

and Firewalls. The Test and Evaluation infrastructure may be collocated or geographically distributed. Amalgamation of different infrastructures leads to scalability and reliability. All these functionalities could be a part of an ideal cyber range as it should have maximum functionalities. However infrastructure does pose negligible complications. Some hypervisors like ESXi is not supported on Cloud infrastructure making modifications in the simulated environment a difficult job. The large environment consisting of hundreds of machines and network nodes needs a lot of effort to create, deploy and control. Introducing new scripts requires efforts, time and learning an altogether different way of working on things. All this consumes a lot of overhead. Even though there are certain challenges concerning infrastructures in a cyber range, it is still an indispensable parameter, making its requirement for an ideal cyber range the maximum. The unquantified value assigned to infrastructure for this very reason is Very High.

- **Scenario (Teams)** - As highlighted in the introduction, the different teams is red, blue, white, purple, green, grey and yellow. Each has its own specific requirement in a cyber range. Bigger the cyber range, more the number of individuals in the team. The Red Team's attack is instrumental in discovering the loopholes in the system. It can be done by sending malicious traffic such as network attacks and spywares. The Blue team is responsible for managing network infrastructure by using antivirus, application servers within a physical

device. This acts as counter mechanism for patching the system and strengthening it to thwart future attacks. The green team simulates users and good traffic accessing applications hosted on network infrastructure managed by the blue team. The purple team sets objectives regarding the offense and defense in the cyber range. The white team monitors critical infrastructure components using Domain Name Service (DNS), intrusion detection systems, traffic simulators and application servers. A cyber range provides platform to carry out all the essential team functions. All these teams are crucial for the cyber range environment, hence making their requirement Very High for an Ideal Cyber Range.

- **Simulation Environment** - A cyber range should be capable of simulating the entire Internet and supporting operations. The process of simulation varies for different cyber ranges owing to the need of the environment. The Florida cyber range uses the Metova simulation platform. The Baltimore cyber range uses Cyberbit simulation platform whereas the Department of Defense cyber range uses Tintri platform. Since the cyber ranges are concerned with providing real life scenarios for training and testing, simulators are an important element for cyber ranges. Training through simulation can assist in analysis of confidential data as well as the decision making processes. Cyber ranges usually deal with three kinds of simulation: real simulation, virtual simulation and constructive simulation. While real simulation is carried out on real systems in form of

cyber exercises in a physical environment of isolated networks, virtual simulation deals with assessment of practical, control and cooperation capabilities by simulating real systems. In constructive simulation, simulated systems are operated by simulated objects [11]. Simulation tools can enhance traffic fidelity, asset analysis and virtualization capabilities. Hence, simulation is a very crucial aspect for cyber ranges thereby making its requirement Very High for an ideal cyber range.

- **Tools**- Based on the environment features of different cyber ranges, different tools could be deployed. Sophisticated tools like Systems Administrator Simulation Trainer (SAST) and A Network Traffic Synthesizer (ANTS) are deployed in polished cyber ranges like National Cyber Range to carry out intense cyber training and testing whereas cyber ranges like Virginia incorporate tools that are easily accessible to students. Baltimore cyber range relies on Security Operations Centre (SOC) tools. Basic tools like Wireshark and John the Ripper could be embedded into the operating systems whereas forensic tools like Encase or Sleuth Kit are easily obtainable. Baltimore Cyber range uses network tools in a hyper realistic virtual network environment. Several tools can be used in cyber ranges depending on the offensive and defensive nature of the training and testing carried out. Tools are an important component of cyber ranges which makes their requirement Very High.

- **People Involved**- Based on previous categorization, we can highlight that cyber ranges are not restricted to a certain group of people ,rather interest different groups of people. Cyber ranges may be accessed by students, professionals, customers, staff, government officials, military, researchers , law professionals etc. The ranges which may support multiple servers, tools and platforms mostly allow remote access which eliminates the need of individuals being directly involved. Significant personnel like a range admin or other technical staff are an indispensable component of the cyber range, and will be directly involved with the cyber range under all the circumstances technically. However people who just access the cyber range may not be directly involved with the range under all circumstances and may also be accessing it remotely, which makes their necessity within the cyber range Low.

- **Automation**- Being mission critical investments and organizations, cyber ranges need to support a large number of devices, network traffic, servers and operations. An automated environment can bring out the best in a cyber range by strengthening the stability, security and infrastructure of the cyber range. Automation can also lead to rapid setup and teardown of test environments. Cyber Ranges like Raytheon rely heavily on automation. The automation software in Raytheon leads to rapid creation of test infrastructure for topology with the need to patch the system every time [12]. DoD cyber range reinforces

automated environment control and provisioning [11]. In the National Cyber Range, automation process verifies the configuration of all devices in the test environment. Automation leads to testing of complex cyber range environments. Thus automation is very essential for cyber ranges making its requirement Very High in case of an Ideal Cyber Range.

- **Performance**- Cyber ranges may deal with high traffic websites simultaneously. If overloaded, the servers may degrade the functioning of the cyber range. Load balancers can deal with such kind of interruptions by efficiently distributing traffic among multiple servers thus balancing the load. For cyber ranges running operations on cloud across multiple servers, real time visibility is a must. Visibility can also help understand resource allocation and if additional resources are needed. Load balancing is not difficult and it provides high availability. Load balancing depends on the size of cyber range and the number of platforms and tools it supports. Since a cyber range supports multiple devices, servers and operations, the performance requirement is Very High.

- **Virtual Clone Network** - The Virtual Clone Network (VCN) aims at providing realistic environment along with training and assessment. It takes into account risk management and hypothesis testing for real time cyber incidents. Comparative analysis of present solutions lead to better solutions for

future. Pen Testing and range based cyber exercises are an additional feature. A cyber range with a Virtual Clone network would be relatively more efficient as VCNs are not restricted to small networks and ensure scalability and reliability. However, Virtual Clone Networks consume a lot of resources and their reliability is a question, making their requirement fall into the Medium category.

- **Virtual Private Network**- A Virtual Private Network (VPN) can connect a machine directly to the management range. VPN is configuration dependent. Cyber ranges like Cisco and DoD encourage VPN deployment for enhancing security and better performance. VPN is excellent for sharing files and remote access. Since security deals with masking of Internet Protocol (IP) addresses, VPN may be used to obtain a different IP address. Accessing blocked websites and bypassing filtered content can be achieved through VPNs. Also it allows online anonymity. Since a cyber range must deal with offence as well as defense, VPNs provide excellent mechanism to perform offensive and defensive activities, thus making their requirement High in a cyber range. The reason we have not quantified this parameter as very high is because VPNs may be successfully substituted with other tools and techniques for accessing blocked websites or bypassing contents.

- **Fidelity**- Fidelity is the quality of correctness and obedience. One of the most important parameters, when it comes to operation of cyber range is fidelity. It is a measure of accuracy, correctness and authenticity. High fidelity cyber range environments promote independent and objective testing along with evaluation of advanced cyberspace capabilities. Major cyber ranges like National Cyber Range and Baltimore Cyber Range ensure high fidelity. The National Cyber Range provides high fidelity realistic cyber environment for sophisticated cyber training and testing during all phases of the system life cycle as well as testing of complex systems. The requirement for fidelity must be Very High for an Ideal Cyber Range.

- **Use of Public Cloud Infrastructure** - Ravello's nested virtualization and networking overlay technology make it possible to deploy public clouds in cyber ranges by mimicking real world scenarios [13]. The main idea of deploying public cloud infrastructure in cyber ranges is that it adds an additional layer of hypervisor to provide isolation (for experimentation with malware and other destructive techniques) and self routing . Apart from that it can provide full pre-configured and tailorable cyber ranges as isolated environments. It also leads to network extensibility. However the downside of using Public Cloud infrastructure is that it blocks broadcast, multiple packets and provides access to Layer 3 and above. Many enterprise deployments rely on Layer 2 protocols for their setup. If a cyber range does not rely on Layer 2

protocols and ESXi hypervisor, deploying Public Cloud infrastructure seems ideal. Also cloud infrastructure does not support port mirroring so tapping into certain ports promiscuously to monitor traffic seems difficult. However, keeping in view the usefulness and convenience we quantify the parameter as High for an ideal cyber range.

- **Intellectual Property** - Intellectual Property may be defined as an idea produced by mind due to intellect. The laws of intellectual properties are supposed to be protected similarly as to that of other properties. In cyber ranges, intellectual properties could be in form of scenarios, games or challenges to perform a given task. As a red team or blue team exercise, several challenges could be posed to the user to either break a system or secure it. It could also be thought of as a drive to build an open source system. Most of the cyber are unable to deploy these, however, there are some like Virginia Cyber Range and the Cyber Range at the University of Delaware that do ensure presence of intellectual property in the cyber ranges. The process of Automation is close to that of Intellectual Property, however, on one hand when is Automation requires manual processing, intellectual properties do not. The value assigned to this parameter is Very High.

3.2 Proposed Ideal Cyber Range

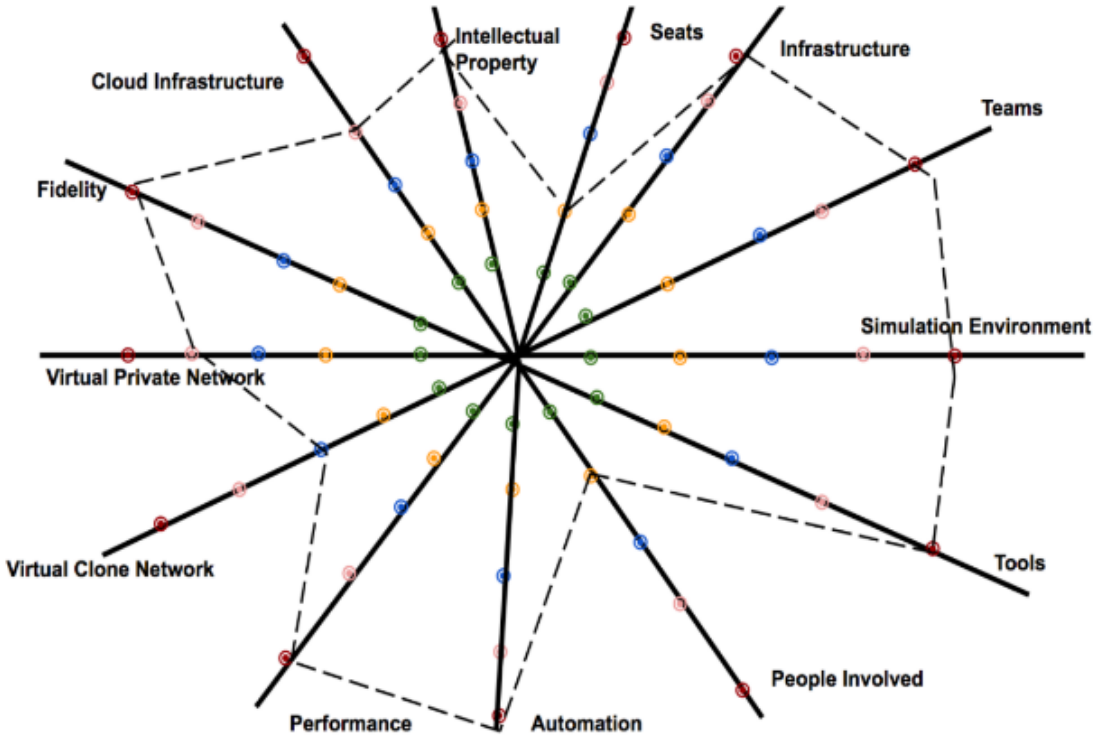
In the previous sections we have highlighted few of the existing cyber ranges. Different cyber ranges have different capabilities. They can be classified on basis of certain parameters that we have already taken into account while describing the important aspects of a cyber range. However not every cyber range exhibits their capabilities based on the parameters. The disparity caused stimulates the surfacing of a cyber range that could take into account all the parameters and become exemplary. We call this cyber range as the Ideal Cyber Range and try to compile it as near to perfect. We attend to the parameters discussed above and based on the requirement level establish a graphical representation. The levels as discussed in the previous sections will be very low, low, medium, high and very high. The representation in form of a table and two supporting graphs is as follows

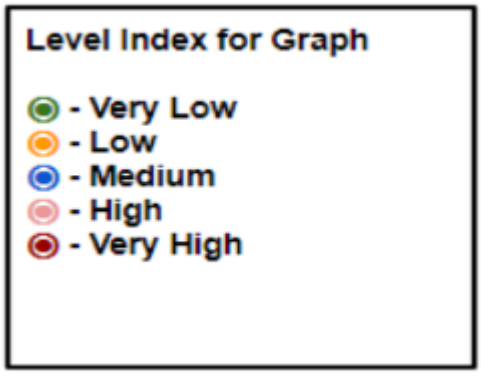
Parameters	Levels
Seats	Medium
Infrastructure	Very High
Scenario (Teams)	Very High
Simulation Environment	Very High
Tools	Very High
People Involved	Low
Automation	Very High
Performance	Very High
Virtual Clone Network	Medium
Virtual Private Network	High
Fidelity	Very High
Cloud Infrastructure	High
Intellectual Property	Very High

Table 3.1: Parameters considered and their priority levels for Ideal Cyber Range

3.3 Representation of the Ideal Cyber Range on basis of parameters

The following is a graphical representation of the Ideal Cyber Range. Each of the lines denote the parameters considered whereas small circular marks are marked inward to outward (very low, low, medium, high, very high) depicting the levels assigned to the parameters.





Index of the Corresponding graph

Figure 3.1: Representation of the Ideal Cyber Range

Alternatively, the graph illustrated above may be represented as follows

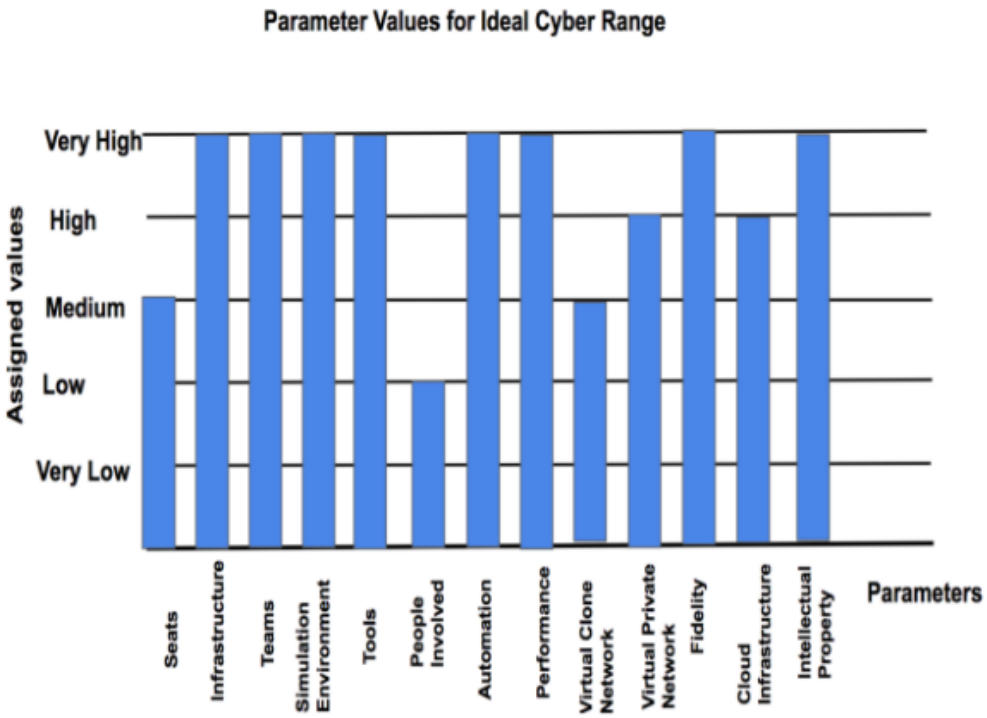


Figure 3.2: Alternative representation showing Parameters for Ideal Cyber Range

The Ideal Cyber Range is based on the significance of the parameters taken into consideration. Parameters like infrastructure, teams, simulation environment, tools, automation and fidelity have very high requirements making them crucial for an ideal cyber range. Different cyber ranges offer different simulation environments in form of virtual machines, hypervisors, sandboxes etc. However an ideal cyber range may adopt hybrid simulation for better functioning. The requirement for performance, virtual private networks and cloud infrastructure is also important although, slightly

low. Number of seats and Virtual Clone Network have medium requirement whereas people being involved has significantly low requirement. We observe that none of the parameters are given a very low priority. While some of the parameters have low requirement, they may still be regarded important for functioning of the cyber range. The requirement for none of the parameters is very low and hence we do not discard any of the stated parameters for an ideal cyber range.

Cyber Ranges have different strengths and weaknesses. We have identified few parameters and based on significance of each parameter we assign a level of importance. This facilitates the introduction of an Ideal Cyber Range with the right values assigned to the parameters in question. Supporting graphs give us a clear idea as to what parameters must be taken into consideration for an Ideal Cyber Range.

Chapter 4

THE CYBER RANGE AT THE UNIVERSITY OF DELAWARE

In this chapter we introduce the newly found Cyber Range at the University of Delaware. The chapter highlights the components and different scenarios of the Cyber Range at the University of Delaware and several attributes like metrics, computing, the simulation platform, tool and teams supported. Since the cyber range is at a very nascent stage, it omits several functionalities as of now. We will also delve into some functionality that is currently being worked upon to enhance the capabilities of the cyber range in future. One such functionality is deployment of the cloud infrastructure. Since cyber ranges support cyber warfare and events like Capture The Flag (CTF), several teams concerned with offence (red) and defense (blue) may be present. We will define the teams that are a part of the range. In the previous chapter, we have considered several parameters that define an Ideal Cyber Range . We will refer to the blueprint of an already proposed ideal cyber range and compare its proximity to the Cyber Range at University of Delaware. This would assist us in determining the strength and weaknesses of the Cyber Range at University of Delaware taking into account what is already done and what could be done in future for the Range in order to become ideal. We rely on different graphs to bring out the variation between the ideal cyber range and the cyber range in question.

4.1 The Cyber Range at the University of Delaware

The cyber range at the University of Delaware was inaugurated on May 2016. The cyber range is facilitated with certain equipments and capabilities in order to ensure cyber defense and warfare training. The cyber range is capable of providing hands on training and exercise, along with classroom training to students and researchers who wish to engage themselves in the field of cybersecurity for the government, military and the finance sector. The cyber range aims to focus on the following.

- **Design and run own training programs** - The cyber range provides virtual facility for testing software and running network simulations. This leads to creation of next generation cybersecurity solutions as new concepts and tools can be tested in a realistic environment. The testing procedure also includes testing of destructive ideas and what-if cases. There are several network tests against malwares. The idea is to test potential weaknesses against networks in the range. The process could effectively lead to generate new tools and techniques and also to test techniques for existing defenses.
- **Provide testbeds for students and researchers**- Students and researchers use the cyber range for multiple purposes. By providing a testbed, cyber ranges improve proficiency and leads to individual and comprehensive assessment. Students and researchers may not only indulge in training and exercises, but can also upgrade their skills and abilities. A performance baseline may be established and the improvement may be tracked on regular basis.

- **Support multiple classrooms in one range platform**- A cyber range constitutes of several tools and techniques which may not be available to individuals easily outside the range. So it provides the perfect platform for classroom and laboratory training for people who wish to gain practical knowledge on the same. Certain programs like penetration testing, system defense and web applications security could be taught in a cyber range environment with plenty of hands on experience on the same.
- **Gamification/Capture The Flag (CTF)-** Since the cyber range is full of networking capabilities, and is capable of coordinating cyber defense and warfare training in the testing environment, it provides the perfect forum for carrying out games in form of Capture The Flag (CTF) contests. CTFs are information security competitions comprising of tasks from certain cyber domains like forensics, web security, penetration testing, etc. Usually the students form groups to solve the tasks.
- In the later sections we will be highlighting the various scenarios that form a part of the cyber range. Apart from that, several components that hold up the cyber range are taken into consideration. Some capabilities of the cyber range are discussed extensively. The cyber range is then mapped to the Ideal Cyber Range to draw out comparisons.

4.2 Various Scenarios supported by the Cyber Range at the University of Delaware

The cyber range is heterogeneous in sense that it can carry out multi facility activities. These activities could range from the basic offense or defense training sessions to advanced open source intelligence techniques. In this section we familiarize ourselves with the feasible situations under which the cyber range operates. The following define some possible scenarios for the CRUD

- **Teams**- The CRUD underpins the concept of teams for carrying out certain activities. These teams could be classified as red, blue and purple depending on the kind of activities they perform. Each of the team has a level of expertise highlighting the levels as demonstration level, beginner, average and expert. The exercises performed could be set upto any level as demanded. Another factor that is considered when teams are taken into account is the size or the scale of the activity. This could be the magnitude of the exercises in terms of the duration or number or set of problems that are a part of each exercise. Finally, the teams also take into consideration the concept of domain. Domain refers to the operating system or environment to which a particular activity or exercise is confined. Functions and operations differ for different operating systems. Thus the teams when working in a cyber range accentuate the importance of level of expertise, scale and domain. The different teams that are observed in the CRUD are as follows.

- **RED** - The red team or the offensive team is responsible for launching cyber attacks on other systems using various attack vectors like viruses, worms, malwares, spywares and other techniques. It simulates real world attacks in order to evaluate the strength of the cyber range and effectiveness of defense strategies applied in the cyber range. Elementary level systems may be vulnerable to a lot of security attacks. The cyber range has taken the initiative to spread cyber security awareness among different masses. High school students and their parents could be given a demonstration of how vulnerable systems are before they are updated and upgraded. Further vulnerable virtual machines like Metasploitable 2 and Kali Linux could be deliberately vandalized to show how attacks perpetuate. An upgrade for the Metasploitable 2 could patch up certain vulnerabilities which could be demonstrated to the masses. After the virtual machine is upgraded, one can easily observe how break ins fail.
- **BLUE** - The blue team in a cyber range analyze systems to ensure security, identify vulnerabilities and verify the effectiveness of defensive techniques. The functions underpinned by blue teams consist of routine log analysis, performing traffic analysis, analyzing data flow and defending the system by system hardening techniques. The overall idea is to defend and harden a system. The performance of a blue team may be determined by the time taken by a blue team to identify the

vulnerabilities and patching up a system. The Collegiate Cyber Defense Competition (CCDC) is a competition that highlights defensive and hardening aspects of a system. Blue team operation may witness two interesting scenarios.

- Blue team identifying the extent of attack performed by Red team in order to patch the system.
- In a situation where systems are identical and different systems have different blue teams assigned, a blue team may discover a vulnerability that is unknown to the fellow blue teams and launch an attack on them.

- **PURPLE**- The purple team is a collaboration of the red team and the blue team and is often the reason for improving cyber defense. In a purple team, there is a combination of red team members and blue team members who work together at every stage. The communication and coordination between the two teams enhances effectiveness and also leads to development of new strategies. It usually consists of expert professionals who are adept in both offensive and defensive techniques when it comes to cyber security.
- **Cross Organizations** - The CRUD encourages cybersecurity training and education not only confined to the walls of the University of Delaware but also beyond that. Capture The Flag (CTF) competitions witness the presence of students and professionals from not only one

organization but several organizations. The competitions may have teams from other organizations like Delaware Technical Community College , Delaware State University or Wilmington University competing with each other as Red or Blue teams to solve certain security puzzles and hence gain cyber security skills and experience.

- **Scanning of machines, ports and Operating Systems** - A network or a machine may be vandalized due to presence of vulnerabilities. Therefore it is important to perform scanning. The cyber range is capable of creating a scenario that would promote scanning. One can scan machines, ports, networks and operating systems in order to identify the vulnerabilities. A network scan takes into account devices with IP addresses (workstations, laptops, printers, routers, hubs, servers, firewalls etc.) as well as the software running. Vulnerabilities like services running in the system and open ports on devices that encourage malicious programs to run invite attackers which ultimately lead to system being compromised. Tools like Nmap may be used to scan and detect operating systems using the technique of TCP/IP stack fingerprinting. Microsoft Baseline Security Analyzer (MBSA) and SecureCheq can scan machines like Windows desktops and servers and provide information about servers, missing service packs and other misconfigurations. Port scanning may be used to analyse network security by identifying open ports that could be misused by attackers. The attackers can exploit such vulnerabilities or run

malicious services on open ports. Nmap, Angry IP Scanner and Netcat are some port scanning tools.

- **Host Vulnerability Scanning**- The idea of host vulnerability scanning refers to automatic host auditing and vulnerability management. It encompasses network mapping, vulnerability assessment and detection, producing reports and remediation tracking. Host based scanners usually perform host vulnerability assessment and may also identify system level vulnerabilities like incorrect file permissions, registry permissions, software configurations and whether policies stated are in accordance. The cyber range is capable of creating a scenario that would anchor host vulnerability scanning. Specific tools like OpenVAS and Nessus can be used to perform Host Vulnerability Scanning.

- **Web Vulnerability Scanning**- Web Vulnerability Scanning must be performed to identify the security loopholes in the Web based applications, which could otherwise be exploited by adversaries in order to gain unauthorized access for stealing confidential information. Web vulnerability scanner interacts with web based applications in order to discover vulnerabilities and weaknesses. Although the real source code is not accessed during web vulnerability scanning, functional testing is performed to identify flaws. The CRUD has the potential to create a web vulnerability scanning

environment on basis of scanners like BurpSuite, Netsparker and Vega. BurpSuite consists of a set of tools that could evaluate the testing process, from mapping to exploiting vulnerabilities. It can assist in monitoring traffic between browser and target application. It is also capable of detecting vulnerabilities, performing customized attacks when needed and for testing the randomness of session tokens. On the other hand Netsparker and Vega can find and report web application vulnerabilities like SQL injection and cross site scripting (XSS). Vega is also used for content analysis and customizing alerts.

- **Exploit Frameworks**- Exploiting frameworks refers to executing of exploit code against a remote target machine. The frameworks usually allow using different exploit payloads in order to obscure shellcode and network traffic. This makes it difficult to be detected. One of the most common exploit framework is Metasploit framework. For the framework to be exploited there are certain steps involved. Initially the code gets into the target system by identifying a bug or vulnerability and checks whether the target system is gullible to the exploit. A payload is configured and simultaneously an encoding technique is adopted so as to get the payload ignored by the intrusion detection system. Finally the exploit is executed. The cyber range can demonstrate the exploitation of framework using Metasploit, by creating the corresponding scenario.

- **Incident responses**- The CRUD is capable of performing incident responses , i.e. in case of cyberattacks, the range can address and manage the consequences. It may also limit the damage and reduce recovery time and costs. Usually an Incident Response Plan is involved in performing incident responses. It consists of procedures that could assist in detecting, responding to and limiting the effects of cyberattacks like denial of services, network intrusions, virus, worms, malwares and insider threats. Incident response incorporates several phases which are preparation, identification, containment, eradication, recovery and final analysis. Although the cyber range has several machines and tools that could participate in each and every phase to ensure incident response, it is important to enforce a communication strategy for better outcomes.

- **Network Forensics** - The computer network is has a plethora of vulnerabilities, which if not attended to could lead to dire consequences. Network forensics is responsible for capturing, recording and analyzing network events. This is done so as to identify the origin of cyber attacks. Network forensics systems are of two types reportedly.
    - Catch-it-as-you-can systems , wherein, all packets passing through a common traffic point are captured so that they may be stored and analyzed.

- Stop Look and Listen systems, wherein each packet is analyzed but only a part of it is stored.
- There are several techniques for conducting network forensics in the cyber range. The range also incorporates several tools that could assist in network forensics. Intrusion Detection Systems which are a part of the cyber range can be used to monitor network activity for questionable traffic. It can raise alerts during security incidents. Similarly, packet capture tools like dSniff, Kismet, Wireshark etc. can capture data that travels over the network. NetFlow data collector can record data passing through monitored devices for a long time. It can reveal information about the source, destination and the volume of data passed.

- **Digital Forensics** - Digital Forensics is analyzing, exposing and interpreting digital data. The idea is to preserve any evidence in its original form, such that structured investigation does not modify it. The digital information is collected, identified and validated for reconstructing past events. The different stages of a digital forensics investigation are acquisition which involves capturing data from computer memory and creating a duplicate so that the original is not modified, analysis wherein an investigator recovers evidence using tools and methodologies and reporting in which the recovered evidence is analyzed to reach conclusions. Digital forensics is performed to identify

where data is stored, preserve the integrity of data, recover deleted files, analyzing the data and perform its documentation to present facts clearly and concisely. Several tools and techniques exist for conducting digital forensics. The cyber range has machines that support many popular digital forensics tools, thereby creating a scenario to perform digital forensics. EnCase, FTK (Forensics Toolkit) and The Sleuth Kit are some digital forensics tools supported by Windows system. While EnCase and FTK used to recover evidence from hard drives, The Sleuth Kit can parse file systems and can examine various operating systems.

- **Penetration Testing** - The CRUD is dedicated towards training and education pertaining to cyber security. It encourages teamwork and organizes cybersecurity competitions to promote cyber security education. Penetration testing is one of the primary skills that cyber security professionals must possess. It is done to evaluate the security of a system. The idea is to exploit vulnerabilities by using certain tools and techniques. The cyber range incorporates machines and environment that support penetration testing tools and methodologies. Penetration testing can be performed keeping in mind a number of steps. Initially, an exploitable vulnerability is identified, followed by an attack design around it. The attack is tested and if successful one of the loophole paths is seized. The attack is launched and the system is hammered.

Metasploit, Wireshark, Cain & Abel, John the Ripper etc. are some penetration tools that can be easily procured.

- **Open Source Intelligence**- Open Source Intelligence (OSINT) refers to any kind of unclassified information and free content that is available over the web. Information may be available from social networks, websites, blogs, forums, etc. It is less expensive as compared to traditional information collection tools. The CRUD can create the perfect environment for OSINT. While some tools used for OSINT are open source, some may be available commercially. Maltego and Recon-ng are inbuilt tools in Kali Linux and are responsible for performing successful analysis for target systems. While Maltego is adept in tracking footprints of a particular entity over the internet, Recon-ng can be used to gather information about a particular domain. Another Kali Linux OSINT tool theHarvester can identify email addresses related to a domain and find the results of hosts and virtual machines in the search engines.

- **Reverse Engineering**- Reverse engineering is the technique of scrutinizing software so that it is easier to identify and interpret what it is composed of. When software is reverse engineered, it is easier to find its weaknesses which in turn lead to better defense strengthening mechanisms. Thus it is an important assignment for both the red team and the blue team. The cyber range provides the apt environment for reverse engineering. Some of the popular

reverse engineering tools are edb-debugger, OllyDbg and valgrind. The edb-debugger is confined to the Linux environment and is relied upon for debugging, instruction analysis, address inspection and plugins. OllyDbg is the Windows equivalent of edb-debugger and can analyze codes, scan files, debug multithreaded operations, recognize ASCII and UNICODE strings, trace program execution, search memory and assemble commands into binary form. Valgrind is compatible with the Linux environment. It can detect errors in memory, perform branch predictions and consists of several experimental tools that can check for array bounds, analyze heaps and generate basis block vectors.

- **Social Engineering** - There are different techniques of conning people in order to gain cyber information. Sometimes it is necessary that the adversary communicates with the target personnel, but social engineering may also be performed without the adversary interacting with the target personnel. Impersonation is one such way, through which criminals successfully obtain confidential information, passwords, networks, devices etc. Social engineering could be classified as a red team task. It could also be used as a means to demonstrate how cyber criminals perform cyber attacks, hence making it one of the significant scenarios in the cyber range. Since the cyber range advertises cybersecurity education, it is important to understand the concept of social engineering which is a crucial cyber security threat. Techniques like tailgating,

pretexting and dumping diving still contribute to social engineering. Sometimes it is necessary to obtain the victim's trust by impersonating others or elaborating a lie, thereby taking advantage of the human element in cybersecurity. Another aspect of social engineering persuades victims to click, open or download attachments which may infect the victims' systems with keyloggers and malwares as well as pilfer their confidential information. The basic social engineering techniques could be easily performed in the cyber range.

- **Spam**- Spam is the techniques of sending undesirable or irrelevant message over the internet recurrently. There are several kinds of spams that exist like email spamming, instant messaging spamming, search engine spamming, classified ads spamming etc. The idea is to spread viruses and malwares in order to vandalize systems, increase views, perform identity thefts or trick individuals. Spamming is an important scenario in the cyber range from the perspective of both the read team and the blue team. As a red team exercise it is nothing but an attack on the target system. As a blue team exercise, one can always deploy spam filters and anti-spam techniques to obstruct the red team adversaries. The cyber range has adequate tools and techniques to create the spam scenario.
- **Phishing and Spear Phishing**- Phishing is a technique wherein targeted victims are approached via electronic mails, telephones or text messages. The

cybercriminal poses as trustworthy entity and lures victims in order to gain sensitive information about the targeted victims. The sensitive information could be in form of passwords, banking details etc. Sometimes spoofed emails seeming to be from legitimate institutions are used in phishing. There are several types of phishing techniques like spear phishing, clone phishing and phone phishing, but spear phishing happens to be the most popular. Spear phishing targets individuals or companies unlike simple phishing attacks where phishing emails are sent to a large number of people, hence making spear phishing attacks difficult to defend. Phishing is a red team exercise and the cyber range is capable of creating such scenario whenever necessary.

- **Authentication**- The technique of ascertaining whether an entity is what it claims to be is termed as authentication. Authentication is not only restricted to humans but also to machines. When a user confirms his/her identity using credentials, it is user authentication whereas machine authentication requires a shared secret like, digital certificate or digital credentials. A cyber range operates through individuals as well as machines, hence making the process of authentication for both remarkable. Be it a red team exercise, blue team exercise or classroom training, at some point of time authentication would be mandatory, hence making it one of the most important scenarios. The process of authentication could be as straightforward as a single-factor authentication or a little rigorous like the multi-factor authentication.

- Single-factor Authentication- It is an elementary authentication technique where a user can easily authenticate himself using a set of credentials like the username and the password.
- Multi-factor Authentication- It is a more reliable method of authentication which uses a combination of what we know, what we are and what we have. What we know refers to a secret code, PIN or password that could identify us against biometrics which represent what we are. What we have is basically something that we possess like a card.
- The cyber range has adequate tools and techniques to verify individuality of users and machines, hence promoting the concept of authentication.

- **Identity theft**- The prohibited act of gathering personal information in order to perpetuate crime is termed as identity theft. The crime could be in form of accessing bank accounts, credit cards etc. There are several ways of gathering victims' personal data.
  - Discarded electronic equipments like computers, memory sticks, hard drives may contain sensitive information.
  - Spywares could be used to obtain personal information by remote accessing target systems

- Unauthorized access can be obtained by hacking/ compromising a system
- Spamming, phishing and other social engineering techniques to gather sensitive information
- Rerouting victims' emails to get sensitive information like bank statements
- A red team exercise, identity theft can be used to sabotage systems. The cyber range has adequate tools, machines and environment to create scenarios that would result in identity theft.

- **Insider threat-** An organization incorporates staff and employees. When a cyber threat emerges from inside an organization and is attributed to the people within the organization, it is termed as insider threat. They could either be intentional (malicious threats) or unintentional (accidental threats), however they are not easy to recognize. The threats could be in form of fraud, information theft or systems impairment. It takes into account certain steps for a successful attack. An insider gets into a targeted system and tries to gain information about the system. Once the insider gains sufficient knowledge about the system, network and the vulnerabilities, he can cause damage with minimal effort. For this purpose the attacker may also rely on setting up a workstation to launch the attack. Thus, in a cyber range insider threat could serve as a red team as well as a purple team exercise.

- **Security Operations Center**- A squad of cyber security professionals who analyses an organization's cyber infrastructure in order to improve it form the Security Operations Center (SOC). They are responsible for prevention, detection and responding to cyber incidents. They usually work in an operational room (war zone or cyber range). They are dedicated towards efficiency, control and visibility of the cyber operations. The technology they rely on is strikingly similar to that of the CRUD, encompassing firewalls, intrusion detection systems, intrusion prevention systems ,security information and event management (SIEM) and breach preventing solutions. They conduct packet captures, event logging and data analysis. The CRUD creates a resembling scenario to that of the SOC and both use web proxies, sandboxes, forensic tools and similar technology components.

- **Log Analysis**- Log analysis is an indispensable scenario for cyber ranges. Every activity performed is a record saved in the log files of the system. Log analysis is conducted for evaluating the records. In case of system impairment, logs are analyzed to comprehend what actions compelled the system to behave maliciously. Thus log analysis can assist in diagnosing system problems in less time, hence leading to effective management. Logs may be analyzed to scrutinize an attack. If an adversary has accessed, modified or deleted data, it would be evident from the logs. Log analysis could be termed as a blue team or

purple team exercise. Every traffic, query, server uptime and error generates log which is extremely useful in system hardening. The CRUD supports a variety of log analysis tools which are capable of functioning either through command line or graphical user interface.

- **Business scenarios** - Business organizations are often hit with cyber security issues. Attacks are launched on business enterprises, industries, banking sectors etc. for financial frauds and for accessing sensitive data. Thus cyber-attacks pose threats and risks to business environments. Therefore it will be fascinating to provide industry domain training programs to young professionals. This would help them prepare against industry oriented cyber attacks which cost millions of dollars and will lead to early detection of such attacks.

- **Anomaly Detection based on Machine Learning**- ne Learning involves analysis of algorithms in order to make predictions on data. The idea is to train a system based on certain training data so that the system can make accurate predictions. Introduction of machine learning to cyber security could be useful in sense that based on statistics and

  Neural Networks tools, the system can make prediction about anomalies all by itself. The system could perform Bayesian learning or Support Vector Machine

(SVM) to detect cyber security related aberrations in a system and add an extra layer of security.

4.3 Components of the Cyber Range at the University of Delaware

Cyber ranges are realistic virtual environments that endorse cybersecurity education, warfare training and development. Since the scope of cybersecurity is tremendous, cyber ranges are equipped with numerous functionalities and operations. The functional and operational aspects of cyber range rely on what the cyber range comprises of i.e. the components of cyber range. Components of cyber range are the building block elements that construct a cyber range. They may be tangible like access points or intangible like servers and databases. Whatsoever be the volume of contribution of the components to the cyber range, they are essential for the overall working. The CRUD incorporates a set of components which we have discussed in this section.

- **Router -** A cyber range witnesses large volume of data flow every moment. A router is a networking device skilled to forward data packets and to direct traffic. Routers are the communication devices over a network and they communicate by relaying of data packets from one router to another router, usually measured by hops. A data packet makes its way from the source router to the destination router by passing through a number of routers. The router gains information about relaying the data packet to its nearest router from the

Routing Information Table which mentions the destination of the data packet. Since the cyber range depicts the network environment realistically, routers form an essential component for the cyber range. The cyber range in question deploys a router named Quagga which underpins routing protocols like Open Shortest Path First (OSPF), Routing Information Protocol (RIP) and Border Gateway Protocol (BGP). Routers function at the physical level of the network. Over a computer network, two kinds of routing behavior are usually observed.

- **Static Routing-** It is a type of routing that requires manual configuration. It is usually performed by network administrator, who simply adds entries manually into the routing table. Static routes mentioned in the routing table are constant and cannot be modified if there is network reconfiguration. Although static routing causes smaller overhead, it lacks fault tolerance and has increased administrative overhead. Cyber ranges do not encourage static routing for obvious reasons.
- **Dynamic Routing-** It is an adaptive routing. Here, the router can decide a route or a destination based on the current network configuration. Sometimes networks face connectivity issues or the issue of damaged networks. In such cases dynamic routing is preferable. Several protocols may be used for dynamic routing. Although the overhead is more in dynamic routing, there is no administrative

overhead. Due to considerable fault tolerance, cyber ranges prefer dynamic routing.

- **Switches**- Similar to routers which connect networks, switches work towards creating networks. They are used to connect devices like computers, printers, phones, servers etc. Switches are thought of as controlling devices which enable other network devices to communicate with each other. They function in the data link layer and are essential components of the cyber range since the range requires devices to communicate with each other effectively. Moreover, switches increase the network bandwidth which is a very useful feature, since a lot of cyber security training and competitions require high bandwidth network. The network performance increases and the workload on individual system decreases due to switches. Another advantage of having switches in the cyber range is that switches may connect directly to the workstations thus reducing a lot of effort. The switches are integral to the hypervisors in the cyber range. It would be fascinating to establish the Snabb Switch into the cyber range hypervisors. They are compatible with the x86 machines and are capable of solving sophisticated network issues.

- **Access Points**- Access Points are found in Wireless Local Area Networks (WLAN). It is a network device (wireless) that acts as a relay point between network devices and the local area network. The existing network coverage

may be extended by means of access points, leading to an increase in the number of users who can connect to the network. The University of Delaware has its own network. A cyber range will have a set of machines, computers, servers and other network devices which are supposed to be connected to the network. Access points enable extended wireless network, so that multiple devices and students may be connected to the network. The Router and the Access Point are connected by a high speed Ethernet cable. This converts the wired signal into wireless signal. Access points allow a broader range of transmission and flexible networking.

- **Domain Name System**- The Domain Name System (DNS) is a means to access information over the internet. To access any webpage, web browsers must communicate with the Internet Protocol (IP) addresses. The DNS is responsible for assigning domain names to IP addresses. Thus it is not mandatory for humans to remember IP addresses. The DNS works by converting a host name into an IP address. Apart from that every machine in the computer network is identified by an IP address, which is useful in finding the device. thus, when a user request a webpage, it gets translated. It is also capable of listing, tracking and matching domain names. Cyber security training, red and blue team exercises and security competitions require access to web pages and are redirected using the DNS service. DNS also allows private servers that are set up covertly by organizations to be available,

although their IP addresses would remain hidden publically. It is one of the salient features of DNS especially in cyber ranges, since teams like red and purple may often need setting up of test servers and networks.

- **VLAN**- A Virtual Local Area Network (VLAN) can be defined as a subnetwork consisting of several workstations, servers and network devices that may seem to be confined to a particular LAN irrespective of their geographical placement. They are usually deployed in busy networks to boost network performance. The devices confined to a single LAN communicate with each other and lead to flexibility due to a centralized environment. VLANs allow scalability, better network management and network security. If the network needs to be reconfigured or the devices and servers need to be relocated, VLANs prove to be useful. VLANs also lead to segmentation and controlling of traffic patterns which is beneficial in cyber ranges, since test networks could be set up using this method, or packet analysis via traffic monitoring could be easily performed. Hence deploying VLANs is a must for cyber ranges. VLANs are easy to set up and require a valid VLAN number, a private IP address and configuration knowledge to ensure communication between devices and VLANs.

- **CDN**- In a Content Delivery Network (CDN), multiple servers and their respective data centers are scattered over a network. It leads to faster

transmission of data which could be in form of files, images, videos etc and also prevents attacks on websites. It is efficient in improving the load times of websites and promoting availability and redundancy which are the highlights of a cybersecurity training environment. CDNs also ensure website security by averting Distributed Denial of Service (DDoS) attacks, improving security certificates and adopting optimization techniques. A CDN works by placing servers at the exchange points between two networks such that the servers are connected to each other, which leads to quick, reliable, secure and cheap data transmission. The internet providers connect to these exchange points for accessing network traffic. The data centers are placed strategically to survive network issues and to impart security across the network. The concept of load balancing is applied to the data centers across the globe which leads to uninterrupted service and ensures that the users can access the website ceaselessly. CDN adopts Secure Socket Layer/ Transport Layer Security (SSL/TLS) certificates for authenticity, integrity and encryption. This guarantees security across the network, making it one of the essential components of the cyber range.

- **Firewall** - A firewall could be thought of as a partition which decides what data packets can pass through or leave a network. The idea is to filter out suspicious traffic in order to prevent malicious traffic penetrating into the network. It works by isolating the system from the network so that every

individual packet may be scrutinized, to allow it to either enter or leave the network. So a firewall is capable of defending a system, validating access into a system, monitor network traffic and sometimes raise alerts in case of doubtful events. The CRUD has a firewall named pfSense deployed as a means of security hygiene. It is open source and can be easily configured and upgraded. Based on how firewalls are installed into a system they can be classified as

- **Host Based Firewalls** - These firewalls are installed into individual systems, servers and monitors. It analyses data packets and determines if a packet should be allowed to enter or leave a system (host). They are flexible in sense that applications and machines can be relocated between different platforms. This allows a device to be configured as required. It also provides internal protection as only authorized persons can access the device thereby eliminating the insider threats.
- **Network Based Firewalls** - Network firewalls are responsible for protecting the network from any kind of unauthorized access. The computer network is guarded against malicious outside access. It is also configured to limit access to external network. It works at the network level by filtering the data that moves from network to a device over the network. Network firewalls offer greater security since security is implemented at the network level. They exhibit properties like scalability, availability and affordability.

Depending on their working, firewalls can be of the following types

- **Packet filtering firewall** - Packet Filtering firewalls work by analyzing packet headers for source and destination addresses, ports and protocols, as a basis to allow them or deny them access into a network. Depending on the predefined policies and rules, IP addresses are matched. If the addresses match, the packet is allowed into the network.
- **Stateful Inspection firewall**- Stateful inspection firewalls perform dynamic packet filtering by taking into account the condition of active connections. Packets that match with active connection are allowed to pass through the firewall. Stateful inspection enforces better security.
- **Proxy firewall** - Also known as Application firewalls, Proxy firewalls are concerned with filtering data packets in the application layer. It acts as a mediator between the servers and the clients. Apart from ensuring which data packets that are allowed and denied into network, it undertakes stateful inspection technology and deep packet inspection technique. They are the most secure firewalls since they do not allow direct connections between the network and the system.
- **Next Generation firewall** - The Next Generation firewall combines the traditional firewall with features like deep packet inspection, encrypted traffic inspection, website filtering etc. They are multi functional but confined to Data Link Layer. They do not have any infrastructure

complexities and are capable of protecting against threats like data leakage and hidden vulnerabilities.

- **Intrusion Detection System** - An Intrusion Detection System (IDS) promotes security of a system by monitoring network traffic for suspicious activities and raising alert when questionable behavior is seen. The IDS may also be capable of detecting malicious activities and thereby performing the appropriate action. If malicious traffic is detected from a particular IP address, the IDS will block traffic from the given IP address. Different IDSs have different methods of performing operations. The following are some of the systems
    - **Host Intrusion Detection System**- In Host Intrusion Detection System (HIDS), security components like firewalls, IDSs, antivirus, firewalls etc are deployed on every system within a network. It monitors hosts, servers, events, logs and key system files to detect system abuse. It is more versatile than the Network Intrusion Detection System. It can take snapshot the existing system for comparing it to the newly taken snapshot to identify if there was any modification. If the system files are modified, it sends alerts and reports to the management.
    - **Network Intrusion Detection System** - Network Intrusion Detection System (NIDS) works by strategic placement of IDSs across a network. This is done in order to monitor and analyze traffic across the network. If a questionable behavior (attack) is suspected, an alert is sent to the

administrator. NIDS have the ability to compare signatures for similar packets. This enables the NIDS to determine if the packets need to be dropped.

The CRUD has deployed two IDSs. They are as follows

- **Snort-** The machines in the cyber range support the Windows, Linux and Unix platforms. Snort, an open source and freely accessible IDS is deployed into the systems (Windows and Linux) in the CRUD. It can analyze traffic in real time and can perform packet logging and protocol analysis. It can search for content and thwart against threats like buffer overflows and stealth scans. Snort can adapt itself into a sniffer, packet logger and IDS. Based on the requirement it will extract network packets, log packets and monitor and analyze network traffic. As an IDS it can also take appropriate action in case of threat identification.
- **Bro**- It is a Unix based open source network analyzer that can be used to build NIDS. The primary functions of Bro IDS are in depth network analysis, assembling network metrics, performing network forensics, traffic baselining etc. Bro has its own event engine and policy scripts. The event engine analyses network traffic and interprets network protocols. The policy scripts on the other hand are responsible for analyzing events to create policies. Bro scripts can read data from files

based on the policies. It is adaptable and highly efficient. Since it has several techniques to detect anomalies, it is quite flexible.

- **Deep Packet Inspection** - Deep Packet Inspection (DPI) is a data processing technique that vouches for an advanced level of analyzing and network traffic management. Conventional packet filtering lacks the ability to reroute packets based on specific data. DPI can detect, determine and classify packets. It can also reroute packets based on specific data or payloads. A combination of Intrusion Detection System and Intrusion Prevention System usually leads to DPI. The procedure takes place at the Application Level and is performed by analyzing packets at checkpoints. The decisions are based on rules and policies and usually take place in real time. DPI can look out for viruses and other forms of vindictive traffic. DPI tools can perform network management by classifying packets as high priority and low priority. Since it performs so many security functions, it ay reduce the network speed. The CRUD has sufficient machines, tools and techniques to carry out DPI.

- **Load Balancers** - The CRUD harbors several machines and servers that are continuously up and running. Most of the time they perform multiple tasks which consumes a lot of resources thus increasing the overall load. If load distribution is not managed properly, the machines may become stagnant and reduce the overall efficiency and performance. Thus Load Balancers are

deployed to distribute workloads across several components of the cyber range. The idea is to optimize the resource usage such that throughput is maximum and response time is minimum. This could lead to an increase in reliability and availability of resources. There are several types of load balancing algorithms that run on basis of different load balancing methods.

  - Round Robin, servers are placed across a network, requests are made to the servers sequentially.
  - Least Connections, servers with least connections to the clients are sent requests. It is calculated on basis of server computing capacity.
  - IP Hash, Servers receive requests on basis of client IP address.
  - Load balancers can handle traffic from HTTP (Hypertext Transfer Protocol), HTTPS (Hypertext Transfer Protocol secure), TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Deploying a load balancer in the cyber range leads to fewer failed components since instead of a single device performing a lot of work, several components perform distributed work.

- **Email** - Sendmail technique is adopted by the cyber range for facilitating internetwork email routing. It is confined to the Unix platform and supports multiple protocols. It may be used as a crossbar switch for relaying messages within different domains. It can perform message header editing since different domains may support different header formats. The configuration is controlled

by the configuration file which may not be approachable. Some of the protocols that Sendmail is based on are Simple Mail Transfer Protocol and Local Message Transmission Protocols. In a cyber range it is possible for servers to be part of different domains. Sendmail techniques can bridge such gaps and act as mail transfer agents to route information over the network to specific recipients. The sendmail may be executed through command line or in a computer-generated imagery (CGI) script.

- **Spam filters** - One of the scenarios that CRUD supports is that of spam. Being equipped with so many machines, servers and workstations, spams are inevitable and the consequences may be critical. Thus in order to protect the enterprise from the unpleasant effects, the cyber range employs spam filters. Spam filtering is a technique that could be used to filter uninvited and undesirable messages, so that it does not access the user inbox. The technique relies on set of particular words and specific content to filter out the messages. However, it may also exclude legitimate emails using this technique, which is why more sophisticated techniques using Bayesian filters or heuristic filters are adopted. They look for word patterns and frequency to filter out spam emails.

- **Virtual Private Network** - Cyber ranges are cyber security provinces with offensive and defensive operations. It is important to secure the communication taking place over the network. Thus CRUD employs Virtual

Private Network (VPN) to add a layer of security for communication taking place over the network. Apart from that a VPN acts as a secure tunnel between network devices and is responsible for protecting the network from being intercepted. Along with securely connecting the devices to the network, the VPN also aids in hiding the IP address and location, only to replace it with an anonymous address. The original IP address in this case gets replaced by the VPN server's IP, such that the footprints can not be tracked. An added advantage of using VPN is data encryption. When the packets are transmitted over the network, they can be easily accessed and intercepted. A VPN provides an AES-256 encryption paired with 8192 bit key for data protection. A VPN also offers the solution to avoid censorship in case one wants to access websites to express thoughts freely. Moreover, VPNs protect WiFi networks, since devices are not directly connected to the network.

- **.Dynamic Host Control Protocol (DHCP)** - With multiple machines and servers within the cyber range, it is important to identify each on basis of their IP addresses. Dynamic Host Control Protocol (DHCP) is responsible for issuing addresses to the machines in the cyber range , which it does based on certain rules and processes. It assigns IP addresses and configures network quickly and automatically. A smaller network may have a router acting as DHCP server, large networks belonging to enterprises witness computer systems as DHCP servers. When a client requests an IP address from the

DHCP server, it issues an IP address for the client to communicate. By assigning the addresses dynamically and automatically, DHCP performs network administration very easily. It relies on the concept of multithreading to process several requests at a given time. It eliminates the need to manually configure the network as well as address duplication. In case there are unauthorized DHCP servers over the network, it can be easily detected due to the assigned IP addresses. Thus employing the DHCP at the cyber range is very convenient to ensure security.

- **Supervisory Control and Data Acquisition** - Supervisory Control and Data Acquisition (SCADA) is an application that is capable of gathering data from a system in order to control it. It also focuses on optimizing the system resources. It could be in form of hardware, software or a combination of both. With a lot of power processing due to multiple platforms, systems and servers in the cyber range, control and optimization are essential to ensure efficiency. Thus he cyber range is equipped with SCADA systems that can directly interact with devices in the cyber range to control them and also extract their events into a log file, thus adding an extra layer of security. These systems can assemble, analyze, process data in real time, ensure redundancy due to their similarity with distributed systems, provide backups and secure alarm systems. Due to its capability of automation, it can easily lead to power restoration.

SCADA can be used to solve issues regarding uptime and redundancy, thus making it one of the significant components of the CRUD.

- **Security** - The range not only harbors components essential for cyber security, but also accommodates components that provide standards security. Since the range is not only limited to being a warzone and also promotes cyber security education and training, it is important to ensure security of students, researchers and academicians working in the cyber range environment. The CRUD ensures safety and security by deploying the following components
    - **Doors and Exits**- The range has multiple doors and exits. In the situation of an unfavorable event, where it is necessary to vacate the cyber range as soon as possible the three doors could be beneficial.
    - **Alarms** - The cyber range is capable of raising alerts when the Intrusion Detection Systems discovers suspicious behavior. Similarly standard security is imposed in the cyber range by installation of alarms.
    - **Fire extinguishers** - Fire protection devices also form a part of security components. In the extremely rare case of the range catching fire, several machines may also get affected. Deploying fire extinguishers could be worthwhile in cyber ranges.
    - **CCTVs**- Closed Circuit Television (CCTVs) or video surveillance technique works by transmitting signals into a monitor, such that the

range can be observed by respective personnel. It can aid in monitoring students and researchers and also for preventing any security crimes.

- **Single Sign On** - One of the important aspects of cyber security is access control. This is related to authentication, such that only authorized entities may access a system. The single sign on property allows users to access independent systems. The idea is to allow a user to access multiple systems within a cyber range using the same set of credentials. Similarly, single action of logging out of a system would terminate the process across all the systems into which the user is logged in. the passwords are not stored and managed externally, hence the risk of accessing third party websites is mitigated. Sometimes, users may find it difficult to remember credentials for different systems, a condition known as password fatigue. Single sign on relieves the users from such condition. Since all the systems can be logged into simultaneously using a single set of credentials, it saves a lot of time. Single sign on can be achieved by a number of system configurations. Few systems adopt ticket generating Kerberos configuration for single sign on, whereas few others rely on smart card based techniques.

- **Web Servers** - A cyber range combines machines, platforms, workstations and servers all running simultaneously. In order to carry out the range operations it is important to ensure that network requests are processes. A web server is

accountable for that. A Web Server could be a hardware or software or a combination of both dedicated towards serving the files which are requested by clients. In other words, it can store, process and deliver the requested content to the clients. The request correspondence takes place over the Hypertext Transfer Protocol (HTTP). As a hardware, a web server may be confined to store files and perform data exchange with the devices over the network. As a software, it can control how users may access certain files. The different web servers that are a part of the cyber range are

- **Static Web servers**- Static Web servers incorporates computer hardware with HTTP server software. The term ‘static’ has been used to exhibit how the server transmits its hosted files as it is to the user’s web browser.
- **Dynamic Web Servers** - Dynamic Web Servers include a static web server and some other software that could either be an application software or a database. The word ‘dynamic’ is used to describe how the application server updates the hosted files and then sends it to the user’s browser, using the HTTP server.
- **E-Commerce Web servers** - E-Commerce Web Servers support E-Commerce hosting. In E-Commerce hosting. Such web servers are used for benefiting commercial organizations. The web server in this case is responsible for allocating components like shopping carts, credit cards

etc. it is equipped with multi channel functionality and service oriented architecture. It can also lead to profile management.

- **Database** - One of the most important virtual components of the CRUD is Database. Information needs to be stored and retrieved whenever required. Database is an organized collection of information that allow storage, retrieval, modification and deletion of data. Apart from that it also supports several data processing functions. The data is usually organized in rows and columns and often indexed for easier retrieval. There are several kinds of databases that the range incorporates. They are as follows
    - **Relational database** - A relational database has data organized in a tabular format, such that it can be rearranged conveniently and retrieved in multiple ways. The data is categorized accordingly, the columns define category whereas the rows define the category instances. Relational Database uses the Structured Query Language (SQL) program. They can be easily extended and do not require any modification for appending data.
    - **Distributed database** - in a distributed database, relevant data is stored at multiple physical locations to promote redundancy. When data is processed at one physical location, the changes get replicated to all other locations. Distributed database can be homogenous in sense that all the physical locations have identical hardware, operating systems

and applications running. Heterogeneous databases have different hardwares, operating systems and applications across multiple locations.

- **NoSQL database** - NoSQL databases are used when there is a large amount of data involved. This is because it is difficult to analyze large volume of data which is unstructured. Sometime the data may be stored in virtual cloud environments. They are non-relational and deliver high performance. Their high availability, scalability and non-resilience makes them highly favorable.

- **Management** - With so many operations taking place inside the CRUD, it is important to manage the range in an efficient and effective manner. The management aspect is taken care by the Security information and event management (SIEM) and the Nagios.
  - **SIEM** - Security information and event management (SIEM) is concerned with real time analysis of the cyber range, and raises alerts when questionable behavior is observed. Two important management features underpinned by SIEM are vulnerability management and identity access management. It can collect data from various sources like logs, servers and databases and look for patterns and common attributes from the data gathered. Moreover, as the events are monitored, it can raise alerts and send reports to the management

whenever malicious behavior is detected. It can store data for a long time and perform forensic analysis on them. It has been known to detect Zero day vulnerabilities. Apart from that, it performs security management by log analysis, log normalization and automatic parsing. It can identify protocol anomalies and can detect covert communications and encrypted channels. The SIEM is known to identify attackers and victims, which make it efficient in cyber warfare detection.

- **Nagios** - Nagios is an application that can analyze a network, system and infrastructure. Similar to SIEM, Nagios can raise alerts when something suspicious is observed. It provides a second alert when the issue is resolved. Nagios is primarily a monitoring tool and can monitor network services (like HTTP, FTP, SSH), host resources, hardware, scripts etc. It can perform remote monitoring and automatic log file rotation. It supports the implementation of redundant hosts, performance data graphing and database backend. It provides information about the network status, history, logs and notifications. It is one of the future prospects that CRUD is considering for better management and an additional layer of security.

- **Employee desktops and laptops** - Although the cyber range is not remarkably extensive and encompasses only six systems, thereby having a capacity of

twenty four seats, it encourages users to connect to the machines remotely or locally, even if the users are not physically present in the cyber range. The students, employees and researchers are entitled to bring their desktops, laptops and devices for cyber security training and competitions. It is a well-known fact that tools are operating system specific hence, tools supported on a single platform may not be supported on another platform. Sometimes users may be curious to understand the working of a specific tool which their system does not support. The department encourages students to explore the cybersecurity domain and spare devices may be provided if required.

- **Cloud** - Operations in a cyber range environment and real life replica of cyber warzone consume a lot of resources. An effective way to overcome this limitation is by deploying the cloud infrastructure in the cyber range. The cloud environment can readily provide a pre-configured cyber range deployed in isolated ranges and increases fidelity. It saves a lot of time by eliminating the need to wait for hardware or setting up a complex environment. It is cheaper than the traditional data centers and can integrate cyber security tools effectively. The CRUD currently does not have a cloud infrastructure as it is at a budding stage, but deploying a cloud environment for the range is an eventuality. At present, there is dedicated scalar supercomputer cluster that minimizes the time and resources cost, but with cloud the efficiency achieved will be greater. The cloud infrastructure being considered for the cyber range is

expected to offload range activities and virtual infrastructure to common cloud computing like EC2, Google Azure etc.

- **Other Hosts** - Apart from the computer systems and devices that are termed as hosts in the cyber range, there are certain other devices that are referred to as the same. A host could be any device that communicates with other hosts over the network. Some of the other hosts in the CRUD are as follows
    - **Host based antiviruses**- They are essential for optimizing the server performance and availability of server. Moreover security issues related to server and server management are performed by host based antivirus which form an important host component for the cyber range.
    - **Endpoint Protection Systems** - An Endpoint Protection System is either a software or an appliance which can be used to identify, manage and control devices that request service or access to the network. They are compatible with appropriate operating systems, antivirus software and virtual private networks. It often relies on client server model and is administered by servers or gateways.
    - **Firewalls** - Host based firewalls are setup on individual devices to monitor traffic in order to determine whether a packet should be allowed into a device or not. It can be configured and customized as per the system requirements.

- **Cyber Security tools** - A cyber range is incomplete without cyber security tools. A variety of tools is supported by the CRUD. The capabilities of tools range from network monitoring to penetrating into a system. The machines support multiple operating systems. Some tools are confined to specific operating systems. Some tools that form a part of the CRUD are as follows
    - **Kali Linux tools**- The Kali Linux platform is famous for conducting penetration testing and digital forensics. The platform is easily available and can be installed into systems with appropriate configurations. It has more than six hundred programs to conduct penetration testing. The platform can be executed through a hard disk, drives, live USBs and virtual machines. It has its own suite of tools that include security tools like Nmap, Kismet, Wireshark, Aircrack-ng etc. Other forensic tools like Foremost and Volatility can be used to conduct forensic analysis.
    - **Open source tools** - Open source security tools are available over the network for securing systems and networks. Some of these tools have been endorsed by security companies and cloud operators. The best known open source tool is Metasploit for penetration testing. Some other open source tools that the range supports are Nessus, OpenVAS and JBroFuzz for network security, Thunderbird and Mailsaurus for protection against emails and spams, TrueCrypt and Cryptology for data encryption and KeePass and CiphSafe to keep passwords safe.

- **Commercial tools** - Commercial tools may be exclusive or freely available. Pwnie Express is one such commercial tool that analyses the network for gathering all information related to the network. It is an excellent tool for threat detection. Aruba ClearPass can be used to access the network and control it. It can identify what connects to the network, enforce policies for appropriate device access and protect resources. ForeScout is a network security management tool that observes devices, administers them and orchestrates responses across data centers and cloud. The process of automation does not require any human intervention.

4.4 Significant Features of the Cyber Range at the University of Delaware

The following are some of the features of the Cyber Range in question.

- **Site Metrics**- The cyber range at the University of Delaware is located in the Department of Electrical Engineering along with the iSuite and Makerspace designed for training and designing engineering artifacts. The site metrics defines the area within which the range is constructed. The range can incorporate six large desks with four seats each, every seat is equipped with computer systems making space for a total of twenty four seats, each an Intel Skull Canyon with 32 GB RAM and 512 GB. Apart from that the cyber range harbors six room displays. The operating system incorporated is Windows 10 and supports hypervisor ESXi. The total room display area measured in square

inches is estimated to be 4x 50" (16:9) + 2 x 70" (16:9). Even though the servers may be remotely accessed, the main idea of introducing seats in the cyber range is to access tools and machines that may not be available to students and researchers outside the range. Sometimes, testing of malwares must be done using sandboxes and hypervisors, which may be readily available in the cyber range itself.

- **Site Computing-** Site computing refers to the operation of computers within the cyber range. Since a cyber range is concerned with multiple tasks, the computers must be highly capable. The computer systems supported by the UD cyber range boast of high quality blades/ servers. There are fifty nine half blades and five full blades in four blade server enclosures. There are fifteen hundred Advanced Micro Devices (AMD) threads. The computing thread speed ranges from a minimum of 2.1 GHz to a maximum of 2.2 GHz. The total computing speed is reported to be 2840 GHz. The total computing memory is 896 GB, whereas the total disk size is 9200 GB. The computing disk speed maintains a constant 100 Mb/sec.

- **Per Seat Metrics**- Per seat metrics define the computational abilities of a single system assigned to a single seat. The display area of each of the computer systems in inches is 1x 34" (21:9). A user may simply connect a laptop to the display for better aspect. Each computing system has a memory

of 32 GB. There are eight Intel threads for each of the systems, with the thread speed measuring up to 3 GHz ensuring that the total speed of the computing system is 24 GHz. the per computer disk size is 500 GB and the disk speed is maintained constant at 500 MB/sec.

- **Environment**- As discussed previously, the range supports virtual machines, hypervisors and intrusion detection system for performing basic cyber range operations which may include traffic monitoring and capturing, traffic generation and classic perimeter isolation techniques. In the components section, we have already been introduced to several components that define the environment of the cyber range.

- **Tools**- The cyber range supports a large range of open source tools. Network tools, operating tools, intrusion detection tools and some encryption tools are available as open source and have been used in the University of Delaware's cyber range for training, testing and security competitions. Kali Linux and Debian Linux based tools may also be sued for network security monitoring and penetration testing purposes.

- **Capabilities**- Capability of a cyber range may be defined as its potential to work effectively. Few features that are responsible for bringing out the integrity in a cyber range are as follows.

- **Real life settings**- By real world settings, we mean hyper-realistic environment and real world threat environments to carry out cyber defense training. It can be done by replicating network setups, using security tools and simulation of network traffic. Such a range is often referred to as a dynamic range.
- **Flexible and Customizable**- A customized cyber range ensures that a user may use the predefined settings and scenario or may even generate custom networks, traffic pattern and attack scenarios. Based on the requirement, tools may also be added to the range. This leads to overall flexibility and the range becomes more and more versatile as per the needs of the user.
- **Fully Automated**- Automation capability of a cyber range ensures stability, security and better performance. Automation takes into account several components of the cyber range such as the operating systems, connectivity, storage and applications and may be used to create large environments in lesser time, hence leading to scalability. Automation also safeguards against rapid set up and sudden breaking down of test environments and constructing a test environment infrastructure without patching it up every time.
- **Controllable Testing Environment**- A cyber range should have a controllable testing environment for supporting the capacity of multiple hosts, client server systems and configurations. It should also be able to

maintain networking, image management, traffic generation, power management and network instrumentation.

- **Reconfigurable Network Architecture**- A reconfigurable network architecture ensures that several hosts communicate. It takes into account packet capturing, protocol analysis and network monitoring. The CRUD promotes the use of firewalls, intrusion detection systems, anti-virus and vulnerability management software.
- **Individual and Team training**- The CRUD provides individual as well as team training. By individual training, we refer to several courses that require a cyber range environment to perform system defense or penetration testing, skills that individuals can hone on their own. Again, specific courses may also require team effort and cyber range may provide an excellent environment for the same. Moreover competitions and hackathons also rely on team work.

- **Cloud Infrastructure**- The cloud infrastructure is believed to be the next big step in the advancement of the cyber range. With numerous functions, operations, components and scenarios, it is important to introduce scalability to the range. One way to increase the scalability of the cyber range is deploying the cloud infrastructure. Components like sandboxes may be replaced by cloud sandboxes to replicate elements for networking, storing and testing. It could lead to hosting of multiple virtual hosts simultaneously without affecting the

performance. Cloud infrastructure poses certain challenges in cyber ranges. One of the issues that the range may face while cloud infrastructure is deployed is the need to modify virtual machines on public clouds since they do not support ESXi hypervisors. Further public clouds do not allow port mirroring which could be crucial for performing certain activities. Although the range does not support any cloud services as of now, it still encompasses dedicated supercomputer-scale cluster. It is believed that some software could be relied upon to eventually offload some range activities and virtual infrastructure to common cloud computing like EC2, Google, Azure, etc.

- **Teams Supported** - Part of the scenario section is the different kinds of teams supported. The CRUD supports three different teams , the Red, Blue and Purple, each defined by the measure of expertise, scale and domain.

- **Federation**- Cyber Range at the University of Delaware is currently known for its educational contribution to students, researchers and academicians. It is currently being researched and utilized for training purposes, and allows multi facility activities. The actual federated operation has not been envisioned keeping in mind the ultra-high security overhead.

- **Fidelity**- The cyber range assures high fidelity. As a quality of faithfulness, fidelity is ensured by usage of tools in the cyber range. These are the same

tools that could be used in a federated environment. The results are correct, accurate and authentic, hence certifying fidelity.

4.5 Comparing the Cyber Range at the University of Delaware with the Ideal Cyber Range on basis of parameters

Previously we have contemplated few parameters in order to design the Ideal Cyber Range. We have already highlighted few important parameters and their significance in the Ideal Cyber Range. Since the parameters explored are not quantitative, we used the qualitative measure of assigning them values from Very High, High, Medium, Low and Very Low. The parameters were assigned these values based on their significance and contribution to the cyber range. In this section we will consider the similar set of parameters and analyze the proximity of the Ideal Cyber Range to that of the Cyber Range at the University of Delaware. We will compare the cyber ranges to observe how ideal the cyber range at the University of Delaware is. We will support our observations using graphs. The following are the parameters considered and their implication in the CRUD.

- **Seats** - The ideal cyber range suggests the importance of seats to be labelled as medium. Certain cyber ranges incorporate more seating compared to the CRUD which encompasses only twenty four seats which is quite low. However the range encourages researchers, professionals and students to

involve their own devices too in the cyber range, hence the cyber range can support a lot many devices than the seats offered. Moreover, as highlighted previously, scenarios like Capture the Flag competitions may not even require individuals to be physically present in the cyber range itself and they can conduct all the exercises and tasks remotely. Thus the significance of seats in the CRUD could be assigned the non quantitative value Medium.

- **Infrastructure** - The CRUD has a robust infrastructure. The firewalls, Intrusion Detection Systems and Deep Packet Inspection provide multiple layers of security. The range incorporates several machines, servers and workstations which perform multiple functions and operations. To bring out efficiency and ensure performance boost, components like load balancers and control devices like Supervisory Control and Data Acquisition (SCADA) are deployed. Virtual Private Networks, Spam Filters, Tools and Single Sign on Techniques guarantee protection and stability of the cyber range. Moreover Security information and event management (SIEM) and Nagios are responsible for cyber range management, thus making the infrastructure reasonably powerful. The Ideal Cyber Range defines the infrastructure as an indispensable parameter, assigning it the value Very High. Since the CRUD has nearly veritable infrastructure, we assign it the value Very High.

- **Scenario (Teams)** - A cyber range scenario defines the various situations that could be created in order to carry out an operation or execute a function. Since the sole purpose of a cyber range is to create a dynamic cyber security environment, some of the components are almost always working. The dynamic environment created by cyber range requires frequent scanning of hosts, networks, web vulnerabilities, operating systems etc. As a training zone, scenarios like business, anomaly detection and log analysis are frequently initiated. Teams like red, blue and purple and individuals taking part in the cybersecurity exercises demand scenarios like forensics, authentication and penetration testing routinely, thus making scenario a significant parameter for the CRUD. The ideal cyber range declared the requirement for scenarios to be very high, and based on the different scenarios at the CRUD, we assign it the non quantitative value Very High.

- **Simulation environment** - A simulated environment may be defined as a replica of some given environment. A cyber range is incomplete without a simulation environment. In order to conduct cyber security training, it is important to create a replica of a given environment, usually referred to as the test environment. This environment is virtual and hyper realistic and allows individuals to conduct tests using tools and techniques, without affecting the actual system. In an Ideal Cyber Range, the requirement for Simulation Environment maps to Very High. However, the Cyber Range at the University

of Delaware is newly found and currently lacks advanced simulation tools. Nonetheless, it is possible to set up machines in order to create a virtual environment. The university offers several simulation tools and virtualization platforms which could undertake the process of simulation. Keeping in view the current status of simulation environment, we assign it the value High. Sophisticated tools and multiple virtualization environment could be deployed in future to overcome the limitation.

- **Tools** - Tools are an integral parameter of the cyber range. In order to impart cybersecurity education, training and skills, it is important to render hands on experience. This hands on experience may not be sufficient if only machines and platforms are provided. In order to carry basic security operations like scanning and sophistication security operations like forensics, security tools are a must. They are operating systems dependent and can be used as for offensive as well as defensive activities. Many tools are open source, so they may not be confined to a particular cyber range, but there are some commercial tools that are restricted to specific cyber ranges. Tools pertaining to Open Source Intelligence (OSI) and Forensics (Digital and Network), two of the important scenarios in the CRUD may not be available freely. Thus the requirement for tools in case of CRUD is Very High. The Ideal Cyber Range also listed the requirement of tools as Very High.

- **People Involved-** Many cyber ranges employ people for security administration. It could be a network administrator or any technical staff, who are mainly concerned with assisting students and researchers in the cyber range, or are involved in restoring the machines in case of technical failures. The Cyber Range at the university of Delaware is limited to students and researchers and is solely established for educational purposes thereby eliminating the need for any technical staff or network admin. The machine and tools are not immensely sophisticated and may be handled by students and researchers engaged in the range. Likewise, the Ideal Cyber Range does not require any staff obligation, thus making the requirement low. However it does support the need for administrator and technical staff. The Cyber Range at the University of Delaware on the other hand, does not have any supervisor, hence assigning the value Very Low to the said parameter.

- **Automation** - Automation is defined as the condition in which systems operate automatically. Some components of the cyber range like the Intrusion Detection Systems and the control systems are capable of carrying out their functions systematically. Load Balancing, Deep Packet Inspection and management using the SIEM all take place automatically. The cyber range is currently devising methods to implement anomaly detection using machine learning, which is again an automation issue. Another project that the cyber range is considering in the coming future is coordinating the elements of the

cyber range using sophisticated scripts. Thus CRUD estimates the non-quantitative level for automation as performance to be assigned the value Very High. Interestingly the same has been seen in case of the Ideal Cyber Range.

- **Performance** - Performance in the world of computing is achieved if a system exhibits any one of short response time, high throughput or low utilization of resources. The CRUD has several components ranging from the basic routers and switches to complex servers and applications. With so many operations running and functions being executed a lot of resource is consumed. Keeping a note of the resources being consumed to ensure better performance, load balancers and control devices like Supervisory Control and Data Acquisition (SCADA) are positioned in the system. Thus performance is termed as an important parameter in the range. The performance for the CRUD is taken into consideration based on the low utilization of resources. This enhances the overall performance of the cyber range, thus assigning the value Very High for the said parameter. Correspondingly, the Ideal Cyber Range requires the Performance Parameter to be crucial, hence the requirement for better performance in the Ideal Cyber Range is also Very High.

- **Virtual Clone Network** - The CRUD does not have a Virtual Clone Network (VCN). A VCN harnesses the capacity from a cloud platform to present a realistic cyber range zone which can be pre-configured and modified

accordingly. They form isolated environments using nested virtualization and software defined networks. It can support multiple devices by extending the already existing networks. VCNs are highly automated and the CRUD is devoid of such functionalities due to non-deployment of VCN. Contrary to their requirement for the Ideal Cyber Range, which defines it as medium, for the CRUD the value assigned would be Very Low due to non-availability of the said parameter.

- **Virtual Private Network** - The Ideal Cyber Range classifies the requirement for Virtual Private Networks (VPN) as high since VPNs may be successfully substituted with other tools and techniques. The CRUD deploys VPN for protecting the network from interception and allowing a secure connection between the network and its devices. Moreover VPNs facilitates location and IP address hiding. All the functions carried out by the VPN can be successfully replaced by other techniques in the CRUD. Secure Socket Layer (SSL) proxy could enable a secure connection along with protocols like Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP). Several tools have the capability to encrypt data. Since so many tasks conducted by VPN may be accomplished by alternative techniques, we cannot classify it as a very important parameter in the CRUD, thereby assigning it the value High, as that of the Ideal Cyber Range.

- **Fidelity** - An Ideal Cyber Range should exhibit high fidelity behavior. High Fidelity Systems have realistic system response during the testing period. High fidelity systems often manifest real time scenarios as in the CRUD. Usually the testing is not influenced by human behavior since the test environments are accurate replica of the real environment. Fidelity defines the authenticity of a device, the CRUD ensures authentication and thus displays high fidelity. Based on the testing environment, sophisticated operations and authenticity, the value of fidelity assigned to the cyber range is Very High, similar to the Ideal Cyber Range.

- **Cloud Infrastructure** - Unlike most of the cyber ranges, the CRUD does not incorporate a cloud infrastructure. Deploying a cloud infrastructure in the cyber range is as good as launching a cyber range in the cloud. The cloud environment will allow flexibility and scalability for configuring and validating real time virtual environments. This would eliminate the need to build a separate physical testing environment. This could save a lot of time and computing resources. The Ideal Cyber Range quantifies the parameter as high keeping in view some of the limitations faced by the ranges with the deployment of cloud infrastructure. Since the CRUD does not deploy cloud infrastructure, the value assigned for the said parameter is Very Low. However, deploying the cloud in future is of quite obvious.

- **Intellectual Property** - Intellectual Property in a cyber range could from anything like a domain name to a search engine. Due to the involvement of red, blue and purple teams, it is necessary to customize the range with scenarios, games and challenges accessible to students and researchers according to their skills. An Ideal cyber Range must have Intellectual Property to ensure that cybersecurity training is emphasized on, assigning a value Very High to the parameter. Correspondingly, the Cyber Range at University of Delaware incorporates intellectual property, thereby assigning it the value Very High.

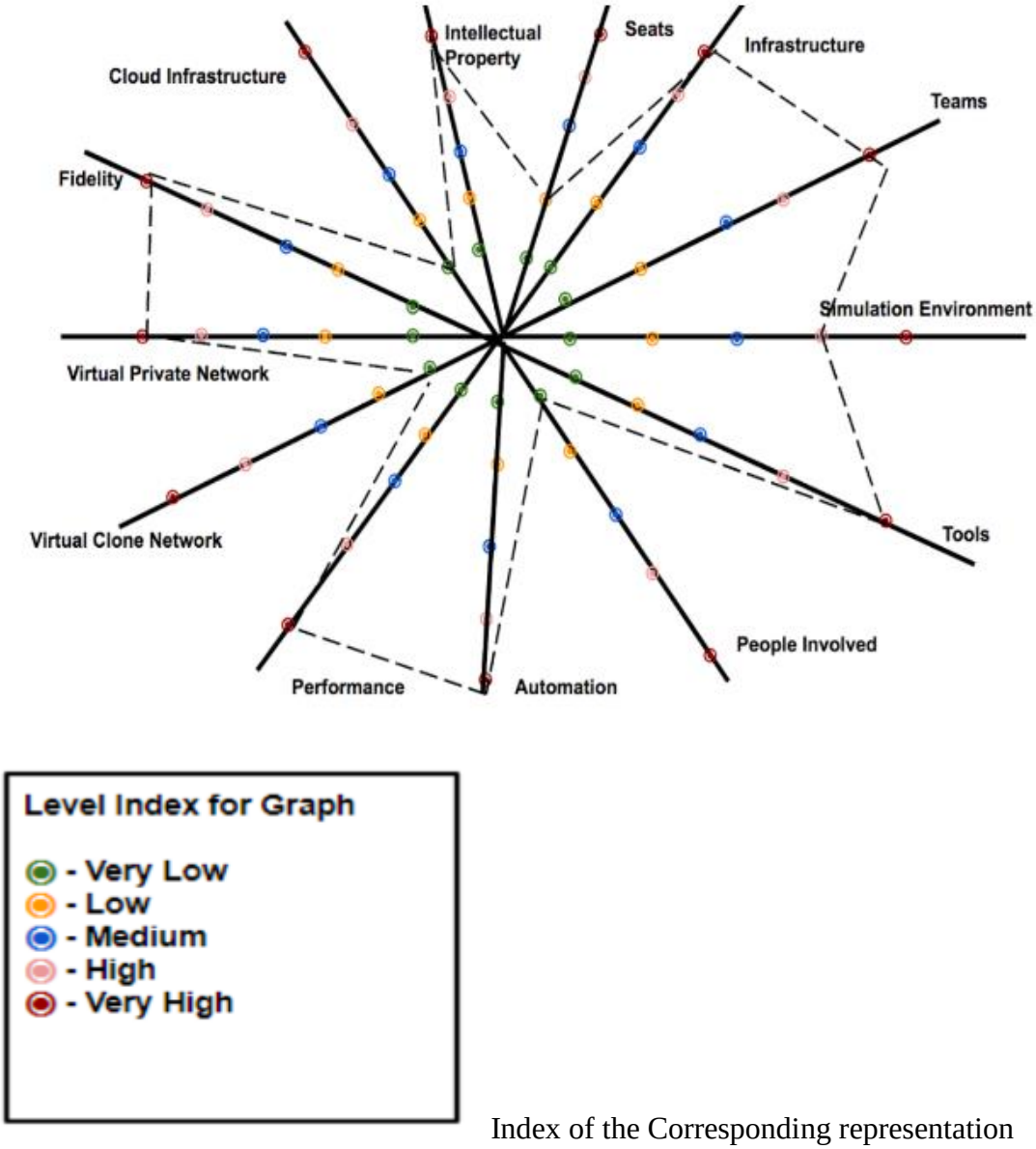
4.6 Representation of the Cyber Range at the University of Delaware on basis of parameters

The previous section describes the parameters, already taken into consideration for the Ideal Cyber Range and the Cyber Range at the University of Delaware. While some parameters manifest equivalent values, there are some which are completely contradictory. In this section, we will produce a graphical representation of the parameters for the CRUD. The representation will be similar to that of the Ideal Cyber Range i.e. including a table and two representations

Parameters	Levels
Seats	Medium
Infrastructure	Very High
Scenario (Teams)	Very High
Simulation Environment	High
Tools	Very High
People Involved	Very Low
Automation	Very High
Performance	Very High
Virtual Clone Network	Very Low
Virtual Private Network	High
Fidelity	Very High
Cloud Infrastructure	Very Low
Intellectual Property	Very High

Table 4.1: Priority levels for parameters in the Cyber Range at UD

Based on the values indicated in the table, we can produce a graph showing the lines as parameters and the levels being indicated in the index correspondingly. An alternative graph has also been illustrated to elucidate the same.



Index of the Corresponding representation

Figure 4.1: Representation of the Cyber Range at University of Delaware

Alternatively, the graph could be explicated as follows. It is a parameters versus Assigned Values graph and the level of value assigned for each of the parameters is comprehensible.

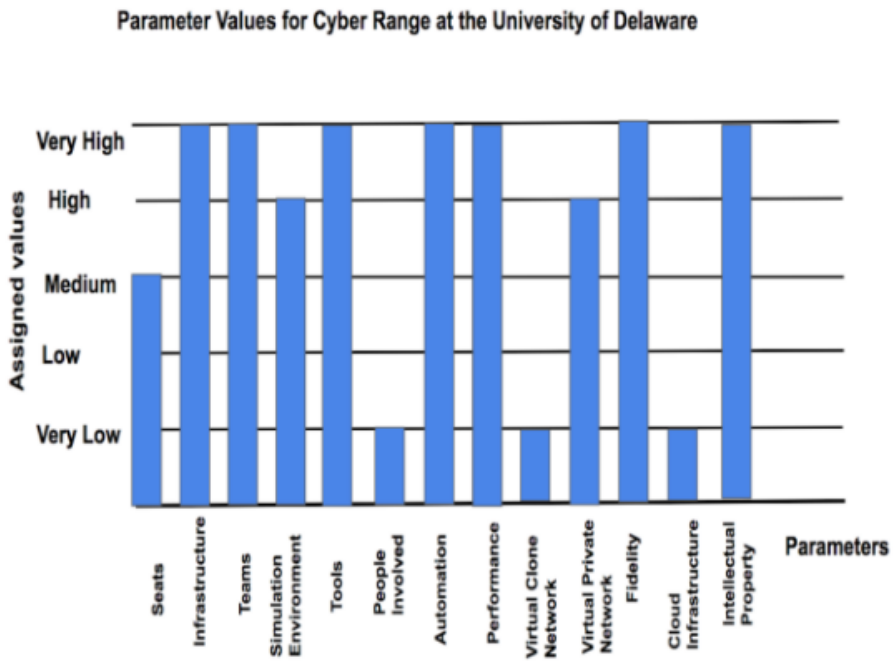


Figure 4.2: Alternative representation of different levels of parameters for the Cyber Range at the University of Delaware

In this chapter, we have come across the newly found cyber range at the University of Delaware. We have highlighted the different scenarios that the range is capable of producing. Also we have explored the multiple components and capabilities that allow the range to function efficiently. Moreover, we have tried to resonate the cyber range with that of the Ideal cyber Range. By taking the parameters that we consider ideal for a cyber range, we have represented the cyber range at the University of Delaware.

Chapter 5

QUALITATIVE ANALYSIS OF THE CYBER RANGE AT THE UNIVERSITY OF DELAWARE

Previously we have proposed the Ideal Cyber Range on basis of Qualitative Values assigned to the parameters in consideration. Taking into account the said parameters, we have attempted to graphically represent the Cyber Range at the University of Delaware to observe the proximity of both the cyber ranges. In this chapter, we will make use of the Qualitative Values to determine the proximity of the two ranges.

5.1 How Ideal is the Cyber Range at the University of Delaware

In the previous sections we have already proposed the Ideal Cyber Range on basis of some significant parameters. We have used the same parameters to assess the proximity of the Cyber Range at the University of Delaware to the Ideal Cyber Range. Although the Cyber Range at the University of Delaware imitates a lot of parameter values compared to the Ideal Cyber Range, there are a few parameters that are altogether divergent. The parameters that have similar values are Seats, Infrastructure, Scenario, Tools, Automation, Performance, VPN, Fidelity and Intellectual Property, whereas the parameters that differ in values are Simulation Environment, People Involved, VCN and Cloud Infrastructure. The values assigned are non-quantitative,

but based on the similar values, we can compute the quantitative value in form of percentage to evaluate the proximity of both the cyber ranges. The percentage proximity may be calculated by given number of similar parameter values divided by total number of parameters whole multiplied by hundred.

% Proximity = (Given Number of Similar Parameters/ Total number of Parameters) * 100

= (9/13) * 100

= appx. 69.23 %

We observe that the Cyber Range at the University of Delaware is at least 69.23 % the Ideal Cyber Range. As the cyber range is expected to deploy Cloud Infrastructure in future, the value is expected to soar.

Chapter 6

CONCLUSION

In this study we have analyzed several cyber ranges and their types. As a part of survey we have taken into account existing cyber ranges and classified them on basis of certain parameters. As we observe that different cyber ranges have different strengths and weaknesses we propose an Ideal Cyber Range using the parameters of classification. Several tables and figures have been used as a means to represent classifications. Based on significance of each parameter we assign a level of importance. Supporting graphs give us a clear idea as to what parameters must be taken into consideration for an Ideal Cyber Range.

Further, we have introduced the Cyber Range at the University of Delaware. As a cybersecurity training and awareness center, the range is responsible for initiating several cybersecurity scenarios which have also been highlighted. For different scenarios to be created, functional components of the cyber range are crucial. Thus the Cyber Range is equipped with tangible and intangible components which have also been discussed. Apart from that, the capabilities of the cyber range have also been taken into account. Previously, an Ideal Cyber Range had been proposed. This study was conducted to map the Ideal Cyber Range to that of the Cyber Range at the

University of Delaware to assess how efficient the cyber range in question is. Although the parameters used to compare both the cyber ranges are non-quantitative, we were able to able to evaluate the proximity quantitatively based on similar and different parameters.

Chapter 7

FUTURE WORK

In this study we have considered a few cyber ranges for analyzing their functioning. Based on our research we have been successful in classifying the cyber ranges into various categories. Moreover, based on the studied cyber ranges we have contemplated some parameters. There are many more cyber ranges which work in a variety of ways, thus increasing the scope for more such parameters in future. Based on the analysis of several other cyber ranges, the level of importance assigned to each parameter for an ideal cyber range may vary accordingly. Since the data collected is not quantitative, the assessment can be only made on basis of logic and conviction. In future, we can delve a bit more into the working of cyber ranges and collect data for a number of cyber ranges to provide quantitative data to an ideal cyber range.

It has been observed that the Cyber Range at the University of Delaware is not very close to that of the Ideal Cyber Range. Several parameters like Cloud Infrastructure, Simulation, People Involved and Virtual Clone Network (VCN) have disparate values for both the ranges, resulting in the differences. While Cloud Infrastructure is being deployed and simulation may be better achieved with sophisticated tools and people may be involved in future, parameters like VCN may not be a part of the cyber range anytime soon. This could escalate the percentage proximity between the cyber ranges

by large numbers. Moreover, new parameters may also be added to the analysis. In the related study section, we came across a lot of cyber ranges affiliated to several Universities. In future, it may be interesting to investigate the parameter values each of the ranges have and assess which range is closest to the Ideal Cyber Range.

REFERENCES

[1] National initiative for Cybersecurity Education, Cyber Ranges, National Institute of Standards and Technology (NIST),US Department of Commerce, 2017.

[2] Standing up a Cyber Range Capability in Michigan Centre for Secure Computing (CSC), De Montfort University Partnered with the Michigan Cyber Security Center (MCC), Dec 21, 2017.

[3] Jon Davis and Shane Magrath, 'A survey of Cyber Ranges and Testbeds', Cyber and Electronic Warfare Division Defence Science and Technology Organisation, Australian Government Department of Defence, 2013.

[4] Douglas A. Solivan Sr, 'Communications-Electronics Command cyber training range launches', Logistics and Readiness Center, CECOM, June 23, 2015, retrieved From https://www.army.mil/article/150996/communications_electronics_command_cyber_training_range_launches

[5] 'Cybershield Training and Simulation, Live training for cyber-security professionals', Cyberbit, 2016, Retrieved From https://www.cyberbit.com/wp-content/uploads/2016/09/CB-TnS-Print.pdf

[6] Standing up a Cyber Range Capability in Michigan Centre for Secure Computing (CSC), De Montfort University Partnered with the Michigan Cyber Security Center (MCC) , Dec 21, 2017

[7] The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime, Critical issues in Policing Series,April 2014.

[8] National Cyber Range, Test resource Management Center, Department of Defense, Feb 24, 2015, retrieved From https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

[9] Martin Gürtler, 'NATO Cooperative Cyber Defence Centre of Excellence', Locked Shields, June 27, 2012, retrieved From https://www.enisa.europa.eu/events/cyber-exercise-

conference/presentations/7.%20Conf%20Paris%20-June%202012%20-%20-%20M.%20GURTLER%20-NATO-CCDCOE.pdf

[10] Corwin Tom, 'Cyber range to be major feature of $50 million Georgia Cyber Innovation and Training Center', The Augusta Chronicle, April 01, 2017, Retrieved From http://chronicle.augusta.com/news/2017-04-01/cyber-range-be-major-feature-50-million-georgia-cyber-innovation-and-training-center

[11] James Curry, 'CyberSecurity Range (CSR) v2.0 Architecture and Capability',Defense Information Systems Agency (DISA), April 2016, Retrieved From http://www.disa.mil/~/media/Files/DISA/News/Conference/2016/AFCEA-Symposium/5-Curry_%20Improving_Cyber_Security.pdf

[12] Raytheon Cyber Range Capability, Raytheon,2017, Retrieved From https://www.raytheon.com/cyber/rtnwcm/groups/cyber/documents/content/rtn_256609.pdf

[13] Baltimore Cyber Range (About), August 2017, Retrieved From https://www.baltimorecyberange.com/about

[14] The Georgia Cyber Range, retrieved from https://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/press_release/Georgia%20Cyber%20Innovation%20and%20Training%20Center.pdf

[15] Roberts Adrienne, DBusiness Daily News, 'Sterling Heights Hub to Offer Cyber Defense Platform for Businesses', February 2016, Image for Michigan Cyber Range Retrieved from http://www.dbusiness.com/daily-news/Annual-2016/Sterling-Heights-Hub-to-Offer-Cyber-Defense-Platform-for-Businesses/

[16] Image for Virginia Cyber Range, Virginia Tech News, retrieved from https://vtnews.vt.edu/articles/2016/09/it_cyberrange.html

[17] Miller Ron, Techcrunch, ' IBM opens new Cambridge, MA security headquarters with massive cyber range' Image for IBM Cyber Range, November 2016, retrieved from https://techcrunch.com/2016/11/16/ibm-opens-new-cambridge-ma-security-headquarters-with-massive-cyber-range/

[18] Image for CRATE, Retrieved from https://www.foi.se/en/our-knowledge/information-security-and-communication/information-security/labs-and-resources.html

[19] Qiu Senior Solutions Architect , June 2016, Cisco Cyber Range

[20] Image for Cisco Cyber Range, retrieved from http://www.manetic.org/images/stories/events/20170424/20170424.JPG

[21] Image for the Cyber Range at the University of Delaware, Retrieved from http://www.udel.edu/content/dam/udelImages/udaily/2017/May/Galleries/isuite/iSuite3.jpg

[22] Image for NATO cyber range, retrieved from https://www.nato.int/nato_static_fl2014/assets/pictures/stock_2017/20170406_170406_NR-3_Robinson_SOC_2_rdax_375x161.jpg

[23] Image for Raytheon Cyber Range, Retrieved From https://www.raytheon.com/index.php/cyber/news/feature/ready-aim-test

[24] Image for Florida Cyber Range, Retrieved From https://floridacyberrange.org/

[25] Tate Emily, Edscoop, 'Regent University opens stand-alone cyber range', October 2017, Image for Regent Cyber Range, Retrieved From https://edscoop.com/regent-university-opens-stand-alone-cyber-range

[26] Reynolds Tom, 'Cybersecurity is focus of new Cyber Range Hub at Wayne State University', January 2017, Image for Wayne State Cyber Range, Retrieved From https://wayne.edu/newsroom/release/2017/01/25/cybersecurity-is-focus-of-new-cyber-range-hub-at-wayne-state-university-6025

[27] Howell Cynthia, Arkansas Online, 'School initiative in Arkansas widens to cybersecurity training' , January 2018, Image for Arkansas Cyber Range, Retrieved From http://www.arkansasonline.com/news/2018/jan/30/school-initiative-widens-to-cybersecuri-1/

[28] Image for Georgia Cyber Range, Retrieved From http://cyber.augusta.edu/au/wp-content/uploads/2017/01/videobgtest.png

[29] Image for Arizona Cyber Range, Retrieved From https://i.ytimg.com/vi/4MpK0wi5CT8/maxresdefault.jpg