University *POLITEHNICA* of Bucharest

Faculty of Automatic Control and Computers, Computer Science and Engineering Department

---

PhD Thesis

in Computer Science, Information Technology and System

Engineering

CR-LM: Cyber Range Lab Manager

ARCHITECTURE AND FEATURES OF NEXT GENERATION CYBER RANGE

presented by

Drd.ing. Dragos-George IONICA

supervised by

Prof.dr.ing. Florin POP

2021

Bucharest, Romania

ACKNOWLEDGEMENTS

I hardly imagine completing my work without the help of so many well specialized people. I don't want to name them all here because I cannot thank them enough for their help. I want to give my gratitude to Prof. Florin Pop, Prof. Ciprian Dobre, Prof. Decebal Popescu and Prof. Nirvana Popescu, my research advisers during the Ph.D. studies, for all their help, support and guidance.

They were always available to give me advice despite an extremely busy schedule. Their analytical understanding helped me through my research studies analytical understanding helped me identify new ideas and scenarios for my research. I look forward to collaborate with them in the future years in order to put in practice more developments and exercises that can be done for educational purposes.

I want to express my gratitude to all my colleagues from the National Cyberint Center for their unconditional support during my doctoral studies. This thesis was made possible only after many inspiring discussions with them. Their encouragement has been a great source of inspiration in my life. In these years, I feel honored to have met so many wonderful people who inspired me with ideas, challenged me and helped me advance in scientific research.

I want to mention here (the list is far from complete) Mihai Predescu, Aniello Castiglione (University of Salerno), Edouard Ivanjko (University of Zagreb), friends and colleagues from Politehnica University in Bucharest, and so many others.

Table of contents

SUMMARY

Over the past few decades, cybersecurity becomes one of the eminent global challenges due to the noteworthy increase in cyber-attacks records. For the protection of personal data, enterprises, to guarantee a safe environment of work and productivity, it is important to raise awareness about cybersecurity. Cybersecurity learning is essential to avoid ad wares, cyber infection, and to deliver a consolidated solution.

Cybersecurity knowledge and cybersecurity training are encouraged by hyper-realistic computer-generated environments referred as cyber ranges.

The main objectives of the thesis were to study complex architectures and features that can be used in cyber ranges, identify the most used architectures and characteristics in world-wide cyber ranges and their key aspects that can be used to create a next generation cyber range and to identify the advantages in increasing awareness for cyber security departments and critical infrastructure.

Many of the results presented in this thesis are closely related to, or motivated by, practical real-life exercises and challenges that I encountered during my daily activities or tasks. In this sense, my scientific and scholarly contributions concern complex architectures and features that can be used in cyber ranges, evaluation of the proposed scenarios used for cyber training for both red team and blue team operators, how to design an efficient collaborative platform that can simulates attacks from basic infrastructures to critical infrastructures that might contain PLCs or SCADA systems.

The results were published in articles in international journals, books and international conferences.

1. Introduction

This paper presents a quick overview about the existing Cyber Ranges and the computer network operations testbeds meant to bring improvements in cyber security training. The current introductory chapter gives a brief on the problem area where cyber developments within the Ministry of Defence (MoD) are introduced along with the test range. The research goal is introduced as well as the study limitations and desired results. This chapter is based on **Cyber Defence Capabilities in Complex Networks.**

The problem area

In its plans for cyber training and defense, the Ministries of Defense of several countries considered its massive cost reduction for its operation, and its desire was getting towards the field of digital resilience and cyber operations. There are some examples of governments, like UK Government and Netherlands Government, that dedicated around €50 million to invest in the field of digital resilience and cyber operations to be used to reinforce the kinetic weapon arsenal in 2016 [1].

From the US Government perspective, that can be generalized, the strategy of an well prepared MoD's cyber component has six objectives:

1. realize an cohesive approach and some good assessments from a cyber security PoV;
2. increase the cyber security resilience of the MoD and other critical infrastructures;
3. development the MoD's capabilities to execute cyber operations (both offensive and defensive);
4. develop more intelligence capabilities in the cyber domain;
5. develop knowledge and acquire innovative capabilities in the cyber security field;

The future governance framework structure of MoD will be the one above [2]. The first entity in the structure is Cyber Command which will take over the cyber operations. The second entity will be cyber operations that contains the intelligence capabilities, defensive capabilities and offensive capabilities. The last entity is the Cyber Expertise Center that concentrates on the skills and the knowledge regarding the cyber operations in the MoD. This entity then will provide a cyber test range (CTR).

The research goal

The research main goal is to design a roadmap for the development of a cyber test range, to study complex architectures and features that can be used in cyber ranges, identify the most used architectures and characteristics in world-wide cyber ranges and their key aspects that can be used to create a next generation cyber range and to identify the advantages in increasing awareness for cyber security departments and critical infrastructure

Thesis outline

In this thesis focuses on cyber ranges, their various applicabilities on cyber trainings through various attack and defence scenarios. It also contains a detailed analysis of several cyber ranges and their types. During this research we identified different cyber ranges that have distinct strengths and weaknesses, so we were able to create an Ideal Cyber Range using classification parameters.

In **chapter 2** we described in detail the cyber operations on Cyber Defence Capabilities in Complex Networks and which are the main components of a MoD Cyber Range. This chapter also includes a comparison between US Cyber Test Range, NATO Cyber Range (CCD COE Cyber Range) and UK Cyber Range.

In **chapter 3**, we described the roadmap for a cyber range, the priority for the cyber range business functions according to the perspective of cyber operations capabilities and the necessary requirements to deliver the business functions.

Chapter 4 introduces the need of realism for cyber ranges and the implementation of attack-defence scenarios based on trending attacking vectors.

In **chapters 5 and 6** we introduced the concepts of physical cyber range and virtual cyber range and we described the architectures of a complex virtual cyber ranges and the various topologies that might be implemented in different types of red team-blue team scenarios.

Chapter 7 introduced the concept of a next generation cyber range and described the essential parameters that can define the perfect cyber range (seats, infrastructure, scenario, staff involved, simulated environment, tools, automation, performance, VPC, VPN, fidelity and intelectual property).

In **chapter 8** we highlighted different components, circumstances, and characteristics like computing, metrics, tools, teams, and platforms of the Cyber Range from the CyDEx Annual Exercise. We also made a comparison between CyDEx cyber range and the perfect cyber range concept.

In **chapter 9** we described the need of cyber exercises for employers that are involved in critical cyber infrastructures like SCADA systems. We discussed about security concepts in SCADA systems, the attacking vectors and the defence perspective.

Chapters 10 and 11 include two complex scenarios that were developed in real-world cyber exercises, on NATO Cyber Coaliton and CyDEx. Those scenarios were targeting complex cyber infrastructures, SCADA systems affected by disruptive attacks and military environments that were affected by fileless malware. Both scenarios include attacking vectors, investigation steps for analysis and recommendations to protect against this kind of attacks.

2. Cyber operations

This chapter presents the most relevant cyber operations from a cyber-range and is based on **Cyber Defence Capabilities in Complex Networks**. Cyber (space) operations are defined as "*the employment of cyberspace capabilities where the main purpose is to achieve military objectives or effects in cyberspace or through it*".

NATO uses the following definitions to describe the capabilities within Cyber Operations:

- Computer Network Operations (CNO) - Computer Network Operations (with three components Computer Network Attack, Exploitation, and Protection) focused to obtain unrestricted access to computer networks to disrupt or deny their capabilities, or use them like a bot.
- Computer network defense (CND) - Actions to protect against denial or destruction of information located in computers, computer networks or the networks themselves.
- Computer network attack (CNA) - Action taken to deny/destroy information from computers, computer networks.
- Computer network exploitation (CNE) - Action taken to make use of a computer or computer network and the information located on them, in order to gain advantage.

The Cyber defense aims at protecting own networks and systems. The Cyber offence aims at disrupting, denying, degrading, or destroying networks and systems [3]. The activities conducted in the cyber-attacks (offensive) and intelligence are similar and they aim at accessing the system to lead to a planned effect. These activities consist of: *recon, scan, access, escalate, exfiltrate, assault, sustain, and obfuscate*.

The activities conducted in the cyber defense follow the life cycle of an incident and consist of six main activities that are part of the NATO Framework: malicious activity detection, attack termination, preventionor mitigation, dynamic risk damage or attack assessment, cyber attack recovery, timely decision making and the cyber defence information management.

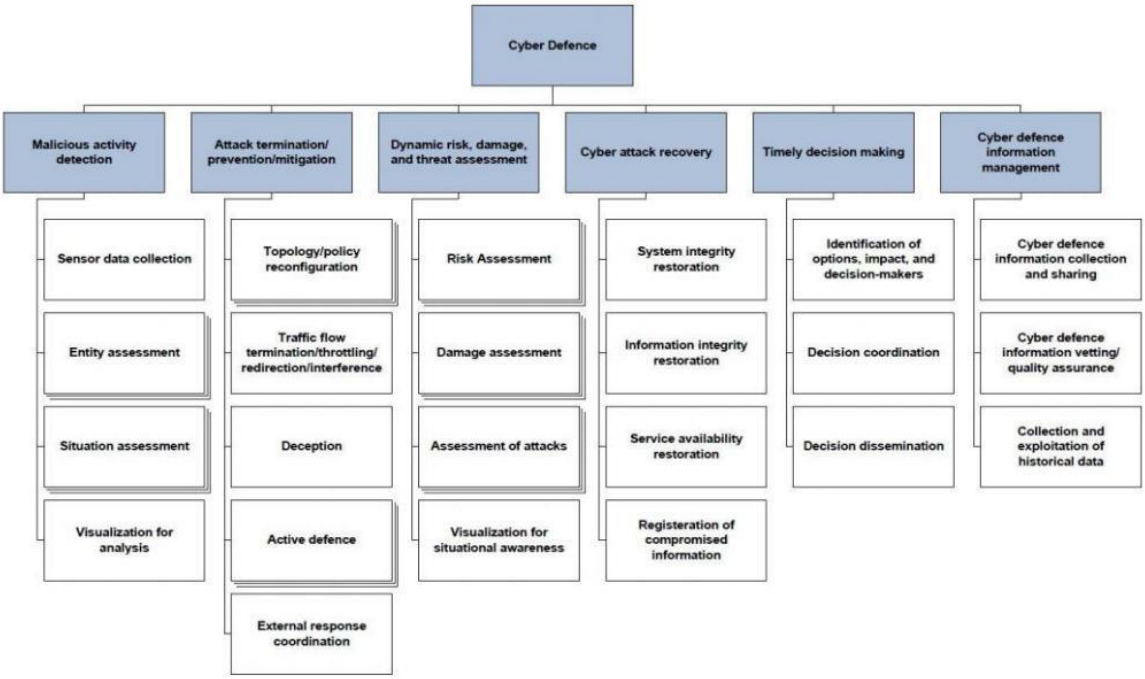

Figure 1. Cyber Defence Capability Framework.

2.1. Developments in cyber test ranges

Cyber test Ranges (CTR) are defined as not-real (virtual) environments used for research, development, evaluation, and training purposes within the domain of the cyber. The aim of the test ranges involves recreating real world situations but without any harm to the real world networks. CTR requirements are demanding. They should replicate the networks and computer systems, imitate the business operations, and produce generate realistic traffic to conduct tests without harming the real environments.

Case studies

There is a various number of CTR that have been made operational or are still under implementation.

These CTR's are good to extract the current or future characteristics and objectives, and in this manner, to add to a superior comprehension of how are cyber test ranges are designed for training purposes to fight against cybercrimes and cyberterrorism.

Examples

1. The United States CTR - The US is in the phase of implementing a National Cyber test Range (NCR). This cyber range will provide the infrastructure and software tools for a secure testing capability to rapidly emulate large-scale complex networks that simulate the depth and diversity of real-world networks. The implementation started in 2008 and will service both researchers and operational users.
In addition to NCR, the US cyber experts started developing in 2006 an information operations (IO) range.

2. NATO - NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) runs a cyber lab, as stated by the Director of CCD COE in an email correspondence. The cyber lab aimed at operational users in support of technical courses for training and technical expertise. In this range are developed two important exercises – Lock Shield (red team vs blue team exercise) and Cyber Coalition [3] (exercise based on different scenarios that involves malware analysis, host and network forensics, traffic analysis and reporting) [4].

3. **The United Kingdom** The UK opened its cyber range in 2010 [5]. Their CTR "is able to simulate a large infrastructures and global threats and evaluate how these networks, whether military, civilian or commercial, respond to an attack in order to develop capabilities that will make these networks more secure".

Northrop Grumman delivers the test range facilities [6]. The cyber range has four common uses:

- Training aimed at preventing falling victim to cyber attacks and response training aimed at improving the handling of cyber attacks.
- To getting and understanding of the robustness of the IT-architecture and to understand the consequences of additions or changes to the IT-architecture
- To test and to benchmark IT-components.
- Research and development.

2.2. MoD Cyber Test Range

The expectations of the MoD business towards the CTR include the CTR business functions that consist of many levels. The first level relates between the CTR business functions with the cyber operations: the functions ease the execution of the cyber operations. The second level is about specific business functions that support one of the capabilities in the domain of cyber operations: defense, offense, or intelligence.

The generic business functions are business functions that support the daily operations and the enable the research and the development. The CTR, to support the operations, try to present business functions that help the personnel to act and assess effectiveness of the current capabilities in the cyber domain. Also, the CTR, to enable the research and the development, attempt to present business functions that help the researchers to carry out the researches into future cyber solutions and to research more when the external solutions enrich the MoD [7].

Exercises are a critical component in cyber security operations as it consolidates each part of cyber operations into a close genuine live action.

Cyber defense/attack - describes the desires towards the CTR from a defensive/offensive point of view. The detailed overview of the cyber defense expectations consists of three components [8]:

- The particular business capacities went for supporting cyber defense/attacks.
- A further specification of the particular capacities into CTR administrations pointed at supporting cyber defense/attacks.
- A breakdown of the CTR administrations into CTR administration segments went for supporting cyber defense/attacks.

3. Roadmap for the Cyber Test Range

This roadmap will last for the next five years, and it includes the delivery of the business functions within the CTR and the needed technical and organization requirements .

To establish the roadmap requires two step. The first step is to identify the priority for the CTR business functions according to the perspective of cyber operations capabilities. The second step is to determine the various levels of the functionalities within a business service and the necessary requirements to deliver the business functions [9].

There are two variables that determine the priorities. The first variable is the urgency (which is the need to use the bushiness quickly) and the second variable is the complexity (which is to know the necessary requirements). Both of these variables (their combination) represents the priorities for the business functions; high urgency and low complexity functions should be conducted first, but low urgency and high complexity should be done next [10].

The CTR maturity model is designed to define the different eves of the functionalities and determine the necessary requirements [11].

4. Real-World Attack-Defense Scenarios for Cyber Security Training

This chapter introduces the need of cyber-ranges in practicing real-world scenarios for cyber infrastructures and is based on the paper **Creating and Managing Realism in the Next-Generation Cyber Range**. To solidify

the versatility of key government, military, and business frameworks, associations are conveying digital extents, inconceivable proving grounds that permit war diversions and reenactments went for fortifying digital security abilities and barriers [12].

4.1. What is a Cyber Range?

The word go in the term digital range is military wording for a run of the mill focusing on or dynamic range where you can send troops to sharpen their battling aptitudes with an assortment of reasonable all around arranged activities that may incorporate connections with weapons and ammo, tanks, war planes, war boats, etc. In that way, the war contender can prepare as they would battle. Digital range preparing concentrates on the best way to assess circumstances and apply the right arrangement/design for particular genuine assault circumstances [13].

It's insufficient just to ensure that things work. They likewise must be strong against assault for an adversary who may be never going to budge on upsetting mission-basic foundation.

4.2. Who Needs a Cyber Range?

Each and every day, the news features shout out about new assaults on the money related industry, monetary extortion, charge card misrepresentation, wholesale fraud, information spillage of corporate privileged insights, safeguard contractual workers being besieged by entrance endeavors, open influence and water arrange interruptions, and politically-or ideologically-roused digital assaults.

In case you're an oil organization whose basic databases are unfavorably changed or annihilated by a digital assault influencing your capacity to deliver your item or to penetrate, then you will completely wish that you had investigated that projection in a digital range environment to have possessed the capacity to successfully relieve it early.

Who needs a digital range? All things considered, it's quite obvious that for all intents and purposes each association needs one. Nobody is safe to these issues and breaks. Each and every day it appears assaults are being disclosed in associations under steady assault.

4.3. Is it Really That Bad?

We consistently know about the steady torrent of new security assaults and the commonness of security gaps. It just appears that there's not a single end to be seen. The way of the vast majority of the associated world makes securing our systems and information in to a great degree troublesome issue to handle [14]. On a par with the biggest programming and equipment advancement companies are, there is by all accounts no limit to the quantity of found security gaps, with security vulnerabilities being revealed every day over the globe for system frameworks IT and administrations.

4.4. How Can We Tackle These Security Issues?

There's been an intriguing arrangement of dialogs continuing for a considerable length of time with contending perspectives in the matter of how to unravel these security issues in both the transient and the long haul. There are examinations about the advantages of open designs, advantages of shut structures, interruption and avoidance frameworks, zero-day assault acknowledgment, bound together risk administration frameworks (UMTS), and a plenty of other security designs and exchanges.

5. Architecting a Cyber Range

The digital range can be architected from multiple points of view however when all is said in done you can aggregate them into three classifications, physical, virtualized, and cross breed. We should investigate every range sort, and their focal points and weaknesses [15].

5.1. Physical Cyber Range Architecture

In a full physical range, you copy your whole physical system foundation, your switches, switches, firewalls, servers, endpoints, and so on. You utilize that copied element for your preparation. This is incredible from a reasonable point of view since you can't get it any more practical than that since you're utilizing fundamentally everything that you're utilizing as a part of your range is genuine.

5.2. Virtual Cyber Range Architecture

In an absolutely virtual range, everything is reenacted. Every segment is copied with virtual machines. This approach offers some particular points of interest. The underlying capital cost and the progressing operational cost are altogether less costly than a full physical reconstructive range.

The range equipment gets to be distinctly easier and that is on account of everything is virtualized to keep running on generally regular off the rack equipment and less master HR, or less master HR, are ordinarily required than for a completely physical documentation. The assault ancient rarities are likewise more effectively discarded. For instance, by returning to known great depiction of your virtualized foundation [16].

Two more cases of why unadulterated virtualization can bring about issues are system throughput, which is dependably lower in a virtualized situation, and firewall IPS/IDS execution which are significantly obliged regarding execution when those components are absolutely virtualized [17].

6. Effective Use of Your Cyber Range

We know we need a cross breed environment and we have a general thought of what we need to virtualized and what we need to stay physical. Since the different segments can be virtual or physical relying upon the preparation situation prerequisites, we won't cover the genuine usage of a digital range inside and out [18], [19]. This chapter is based on the paper **Creating and Managing Realism in the Next-Generation Cyber Range.**

The steered correspondence connections could be anything also: ISP associations, coordinate point-to-point cabling, satellite interchanges, cell, or other. Possibly you have a few servers hanging off of a system neutral ground (DMZ) [20].

A DMZ is an outer venture administration, for example, web facilitating and mail administrations. This may be your openly confronting web and mail servers for instance. They may likewise have unique access through the firewall to other corporate assets and servers, making them most likely focuses for assault by outside systems [21].

A high-level topology of a Cyber Range includes:

- Data-Center: Internal enterprise services (DC, DB, FileServ, Exchange etc.)
- DMZ: External enterprise services (web hosting, mail services etc.)

From internal Clients:

- Surfing the Internet
- Internal clients browsing the WWW
- Internal clients accessing enterprise resources from the data center

From external clients:

- Clients from Internet that are willing to penetrate / harm the organization
- Internet Users accessing DMZ
- DNS and Mail SYNC
- Internal Clients accessing from Internet via VPN

6.1. Technology Development Assessment

How about we first discuss the innovation advancement evaluation case. At first look, this case has all the earmarks of being straight forward. You're utilizing the range to survey execution in a specific gadget or administration under imperatives that you set. Utilizing the range furnishes you with a substantial lab

environment, mapping to genuine utilize cases that you can guarantee your gadget, benefit, arrangement, bug settle, and so forth will act not surprisingly once conveyed to creation.

Same thing would go, in case you're looking at various items in an item bakeoff. Note that authenticity is exceptionally essential in a digital range. In the event that you don't have sensible situations that include reasonable foundation activity and practical security assaults, then your range is essentially pointless [22].

6.2. Red Team/Blue Team Cyber Warfare Training

In preparing situations, it is anything but difficult to perceive how things can rapidly get a considerable amount more muddled. We utilize what we call red groups and blue groups to separately assault and shield the system, servers, and applications as a major aspect of the digital range, surrendered rules set by white group. White groups are critical.

They set the objectives for the work out. These could be red group based objectives, blue group based objectives, or both. They deal with the preparation work out, have full perceivability into the work out, and set the guidelines of engagement. The white group additionally guarantees the requirements in which the preparation practice will happen.

6.3. Zero Day Attacks

Zero Day attacks are a definitive assault vectors in light of the fact that by definition what they allude to are assaults that have not yet been found by security seller specialists. They are engendered by malevolent interests to pick up control of what you believed were well protected organize assets.

They can likewise bring about an interruption or decimation of components of your system or your information. At times such malware can even lay in sit tight for an exact time when they're told to wreak facilitate destruction. You may never know whether or when that happens. They can likewise erase themselves, transform themselves, and do a wide range of other dreadful things in a situation.

6.4. Creating and Managing Realism in the Next-Gen Cyber Range

There are numerous potential digital range arrangements and situations that a very much outlined range can achieve. We've experienced a few situations as of now. What you immediately acknowledged is that every last arrangement requires distinctive human components, scale, and assault and safeguard standards. What you'll likewise discover is that these things devour a lot of HR and set-up, readiness, and examination time, which compare to time and cash. This may make you oblige your activities to the point that they get to be distinctly lumbering and don't yield the outcomes that you need. You can without much of a stretch get overpowered with these basic variables to the disservice of your activities, consequently lessening your adequacy and precluding your benefits from having the capacity to genuinely prepare as they battle.

7. Introduction of a perfect cyber range

In the following chapter, we will discuss a few parameters that are crucial for cyber ranges. Then we will assign qualitative values to these parameters based on their importance to the cyber ranges. These qualitative values will help in offering the perfect cyber range.

7.1. Fundamental Parameters in Cyber Ranges

The performance of cyber ranges is based on specific parameters as they are operation oriented. These parameters range from seats to infrastructure hence impacting the functioning of cyber ranges in some way. A few of these parameters are revealed in this section. Based on these parameters' importance and the gravity of functions, we decided to assign some unquantified values such as deficient, low, medium, high, and very high [23]. These parameters are:

Seats – The size of the cyber range can be defined by the number of systems and seats included. The parameter requirement for cyber ranges could be medium since cyber ranges involve functions exclusive to the ranges [24].

Infrastructure – Cyber ranges own their explicit infrastructure according to their functions. Multiple infrastructures and architectures are combined to create their infrastructure. For this reason, the unquantified values assigned to the infrastructure parameter is Very High.

Scenario – As mentioned earlier, there are various teams, i.e., red, blue, green, yellow, grey, purple, and white, having their particularities in a cyber-range. The Red Team's attack is active in finding the loopholes in the system. All of the crucial team functions are carried out by the platform provided by the cyber range.

Staff Involved – Based on the previous classification, we can conclude that cyber ranges are not limited to a particular group of people; instead, it interests various groups of people. Students, researchers, professionals, law professionals, military, government officials, staff, customers all can access cyber ranges.

Simulated Environment – A virtual cyber-range should have the ability to simulate the whole internet and its supporting operations. Simulators are a significant element for cyber ranges as cyber ranges' primary concern is providing real-life states for testing and training. Hence, making simulation an essential aspect of the cyber range and making its requirement Very High for a perfect cyber range.

Tools – Various tools could be installed depending on the environmental attributes of different cyber ranges. Tools are also an essential component of cyber ranges making their requirement as Very High.

Automation – Test ranges have to support an abundant number of severs, operations, devices, and network traffic as mission-critical investments. Automation may lead to testing complex environments in the cyber range, making automation an essential component of the cyber range and making its requirement Very High [25].

Performance – Cyber ranges sometimes deal with heavy traffic websites concurrently. If it gets overloaded, the servers may negatively affect the performance of cyber ranges. To balance the load and deal with interruptions. The cyber range supports several operations, devices, and servers; hence the performance requirement is Very High.

Virtual Clone Network – This component is responsible for offering a realistic environment, along with training and testing. However, VCNs use numerous resources, and their reliability is an issue itself hence making their requirement Medium.

Virtual Private Network (VPN) – A virtual private network is used for connecting the machine to the management range. It is configuration dependent. VPNs have not qualified for a very wide variety because they can be easily replaced with other techniques and tools for achieving similar goals [26].

Fidelity – Fidelity is the quality of compliance and rightness. It is a vital parameter for the operation of the cyber range. Fidelity measures correctness, compliance, accuracy, and authenticity. For a perfect cyber range, the requirement for the fidelity parameter is Very High.

Public Cloud Infrastructure – The primary goal of a cloud infrastructure deployment in cyber-ranges is to include an extra cover of the hypervisor to provide isolation and self-routing.

Intellectual Property – Intellectual property can be defined as a thought, suggestion, or proposal created by the mind due to intelligence or intellect. Mostly cyber ranges are incapable of deploying intellectual properties. The value of the intellectual property parameter is set as Very high.

7.2. Proposed perfect Cyber Range

In the previous chapters were presented several cyber ranges that presently exists. Each cyber range has its abilities. The inconsistency caused by the development of a cyber-range could allow for all parameters and become a perfect cyber range [27].

Data presentation in the form of tables and graphs are as follow:

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

Table 1. Parameters and their respective priority levels for a perfect Cyber Range.

7.3 Perfect Cyber Range Representation Based On Parameters

A perfect cyber range is graphically represented below. The lines indicate the considered parameters, while small round marks are marked from innermost to outer, indicating the parameters' levels [28].

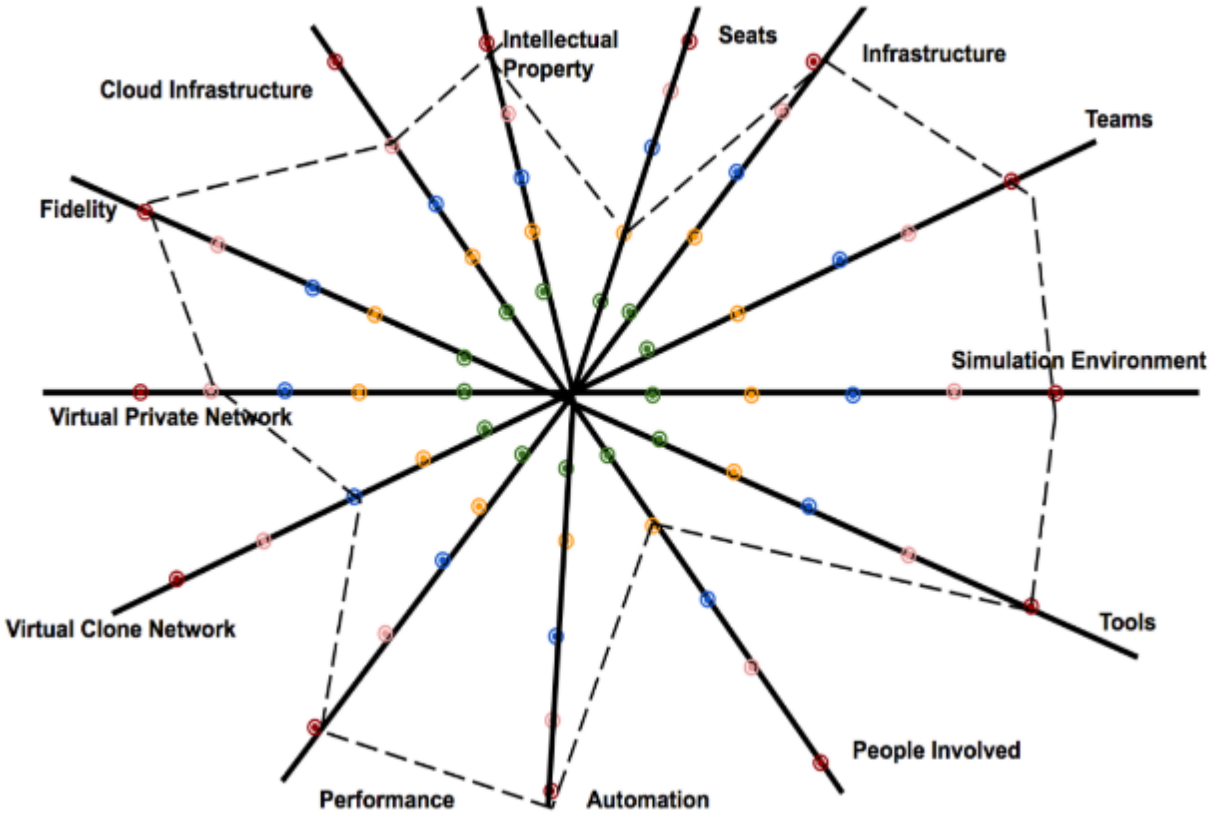

Figure 2. Representation of Perfect Cyber Range [29].

Different cyber ranges provide a variety of simulation environments such as hypervisors, virtual machines, and sandboxes. Nevertheless, for better features and operations, hybrid simulations are adopted for a perfect cyber range. Other parameters, such as VPNs, cloud infrastructure, and performance, are also crucial but slightly lower. We notice that there is no parameter that as requirement shallow. However, specific parameters whose conditions fall in the low category are still considered significant for the cyber range functioning. Also, there is no single parameter with a very low category; hence none of the stated parameters could be discarded for a perfect cyber range [30].

Cyber ranges have unique strengths and limitations. A few parameters have been identified. Based on their significance, we assign a level of importance to them, thus facilitating a perfect cyber range. Graph representation helps us get a clear idea of parameters that need to be considered for an idea of the cyber range [31].

8. CyDEx Cyber Range

In this chapter, we will discuss the Cyber Range from the CyDEx Annual Cyber Exercise. This chapter highlights different components, circumstances, and characteristics like computing, metrics, tools, teams, and platforms of the Cyber Range from the CyDEx Annual Exercise. In this chapter will be described the teams that are the components of the range. This chapter will also contain the blueprint of an already planned perfect cyber range and evaluate its closeness to the Cyber Range from the CYDEx Annual Exercise. [32]. Considering what is already performed and what are the possibilities in the future for this type of range to become ideal for cyber exercises.

8.1. The Cyber Range from the CYDEX Annual Exercise

The cyber range was inaugurated in May 2017 at the National Cyberint Center at first edition of CyDEx. The cyber range is provided with specific equipment and abilities to ensure warfare training and cyber defense. The cyber range can provide exercise and training. The main focus of cyber range is on the following:

Planning and Running Training Exercise - The cyber range gives facility for running network simulations and software testing. This procedure could efficiently lead to the creation of new tools and techniques and testing techniques.

Offer Test-Beds for Researchers and Students- Students and researchers utilize the cyber range for various reasons. This will help to establish a performance baseline and tracking development regularly [33].

Capture the Flag- As we know, the cyber range is filled with networking abilities. It can also coordinate warfare training and cyber defense in the testing environment. These tasks are usually done by the students in the form of groups.

8.2. Scenarios that are supported by the CyDEx Cyber Range

The cyber range is heterogeneous as it carries out various facilities. In this section it will be presented the possible circumstances in which the cyber range operates. Here are some feasible scenarios for the CCR.

Teams- the CCR underpins the idea of teams for carrying out specific activities. These teams include red, purple, and blue based on the activities they execute. There are various operations and functions for various operating systems. Several teams observed in the CCR are as follow:

RED: The RT is accountable for the initiation of attacks on other systems using various vectors such as malware, spyware, worm, or viruses. Basic level systems might be susceptible to many security attacks.

BLUE: The BT in a cyber-range is responsible for analyzing systems to recognize vulnerabilities, guarantee security, and validate the defensive technique's effectiveness. The blue team highlights functions such as traffic analysis, log analysis, and data flow analysis.

The blue team finding the level of attack carried out by the red team in order to fix the system. A scenario where systems are identical and each system are assigned with a different Blue Team [34].

PURPLE: The PT is a partnership between the blue team and the red team and usually the reason for the improvement of cyber defense. The purple team combines blue team members and red team members and collaborates and works together at each stage.

Scanning Operating System, Machines, And Ports-A machine or network can be sabotaged due to the presence of susceptibilities, so scanning is necessary.

Host Vulnerability Scanning – Host vulnerability scanning is usually referred to as vulnerability management and automatic host auditing. The cyber range can create a situation that would fix host vulnerability scanning.

Web Vulnerability Scanning – this actions should be performed for finding web-based application security loopholes. These loopholes can be subjugated by adversaries to get illegal access for theft of confidential information. This scanner helps in checking traffic between browser and application.

Exploit Frameworks – those refer to exploit code execution beside a remote machine considered as target. To uncertain network traffic and shellcode, these frameworks mostly allow the use of various exploit payloads.

Incident Responses – The CCR can perform event responses such as cyber-attacks; the cyber range can deal with the consequences. It can also limit the damage and decrease mending time and costs. An Incident Response Plan comprises procedures that can help identify, react, and restrict the effects of cyberattacks such as virus, worms, network intrusion, malware, and threats.

Network Forensics – A network is an enormous accumulation of vulnerabilities, which can lead to terrible outcomes if not attended. There are two types of Network forensics systems.

Digital Forensics – is responsible for digital data analyzing, revealing, and interpreting. The primary goal is to conserve any proof in its original form to not be tailored by structured exploration.

Penetration Testing – The CCR is devoted to education and training regarding cybersecurity. It motivates joint effort and arranges competitions for cybersecurity to endorse cybersecurity education.

Open Source Intelligence – this is usually referred to as free content and unspecified information available over the web. This information might come from websites, blogs, social networks, forums, etc.

Reverse Engineering – is an analysis technique to analyze software to make it easier to find and interpret what it is made of. The cyber range gives an appropriate setting for reverse engineering.

Social Engineering – There are numerous techniques to cheat or defraud people to cyber information. Sometimes communication between adversaries and the target personnel are needed to perform social engineering.

Spam – Spam is the method of sending an unwanted or inappropriate message over the internet repeatedly. Various spamming types exist, such as instant messaging spamming, email spamming, classified ads spamming, search engine spamming, etc.

Phishing and Spear Phishing – The cybercriminal fakes as an honest entity and entices victims to get sensitive data about the besieged victims. The sensitive data could be in the form of banking statements, passwords, etc.

Authentication – A cyber range works through users and machines, therefore making the procedure of authentication outstanding for both. Whether it is a classroom training, red team exercise, or blue team exercise, the authentication would be necessary at some instant, hence it is one of the most important scenarios.

Single-factor Authentication – User can simply authenticate himself through this method by using a pair of credentials i.e. username and the password.

Multi-factor Authentication – This technique is more reliable, which utilizes a mix of what we have, what we know and what we are. What we know means a secret code, password, or PIN, which can find us against biometrics, which symbolize what we are.

Insider Threat – it reffers to a cyber threat that appears from inside an organization and accredited to its people. These threats could be intentional, i.e., malicious threat or unintentional, i.e., accidental though they are difficult to identify.

Security Operations Center (SOC) – is a cybersecurity expert team that examines an organization's cyber infrastructure to improve it. They are responsible for avoidance, recognition, and responding to cyber events. They generally work in an operating room (cyber range or war zone).

Log Analysis- this is a basic state for cyber ranges. Each action performed is a record secured in the system's log files. Log analysis is performed to analyze the records. In the case of system, weakness logs are examined to understand what activities constrained the system to act malevolently.

8.3. Components of the CyDEx Cyber Range

Cyber ranges are realistic virtual settings that promote cybersecurity learning, combat teaching, and development. Since the range of cybersecurity is incredible, cyber ranges are prepared with several functionalities and procedures. The cyber range's functional and procedural features depend on the cyber range, i.e., cyber range's components.

Router – in a CR can be observed a huge volume of information flow each second. A router can be defined as a networking device expert to direct traffic and forward data packets.

Switches – those work towards forming networks, just like routers that connect networks. They are employed to link devices such as mobiles, computers, servers, printers, etc.

Access Points – those are often located in Wireless Local Area Networks (WLAN). Access Point is a network device that proceeds as a transit point between the local area network and network devices.

Domain Name System (DNS) – is a way to access data over the internet. To access webpages, communication is required between web browsers and Internet Protocol (IP) addresses. The DNS is accountable for allocating domain names to IP addresses.

Virtual Local Area Network – VLAN – is defined as a sub-network comprising of various servers, workstations, and network devices that may appear to be limited to a specific LAN regardless of their geographical position.

Firewall – this could be an idea of a partition that chooses what data packets can pass through or depart a network. The thought is to filter out doubtful traffic to avoid malicious traffic transmission into the network.

Intrusion Detection System – the IDS ensures security by monitoring network data for suspicious activities and issuing alerts when questionable activity is discovered. It may sense malicious activities and take appropriate action against it.

Host-Based Intrusion Detection System – In this kind of system, security components, e.g. IDSs, antivirus and firewalls, are installed on every system inside a network. It observers logs, events, servers, hosts, and critical files of the system to identify system abuse.

Network Intrusion Detection System – It functions by strategic placement of IDSs all over a network to evaluate traffic and data movement across the network.

Deep Packet Inspection (DPI) – is a data filtering technique that inspects a high level of analysis and network traffic control. Traditional packet filtering cannot reroute packets based on particular data, whereas DPI can detect, control, and classify packets.

Load Balancers – The CCR marinas numerous servers and machines which are always running. Generally, they carry out multiple tasks that require many resources, therefore increasing the load.

Email – The cyber range has adopted the technique of sending mail to facilitate internetwork mail routing. It is limited to the UNIX platform, and multiple protocols are supported by it.

Spam Filters – are one of the scenarios which are supported by CCR. Being connected to many workstations, servers, and machine spams are unavoidable, and the consequences may be severe.

Virtual Private Network – To secure the network's commination, cyber ranges must have both offensive and defensive operations. As a result, CCR uses a Virtual Private Network (VPN) to ensure safe communication across the network.

Supervisory Control and Data Acquisition – It could be in the form of software, hardware, or a combination of the two. High power processing is required due to the numerous systems, platforms, and servers in the cyber range, so ptimization is essential to maintain efficiency.

Security – Both components are present in the range, including one that is essential for cybersecurity and those that provide standard security. Because the cyber range is not limited to a warzone and indorses training and cybersecurity eduation, it is necessary to ensure the safety of researchers, students, and academicians.

Exits – There are multiple exits on the range. The three doors could be useful in the event of a negative or unpleasant incident where it is necessary to vacate the online range.

Alarms – Intrusion Detection Systems can use the cyber range to set off alarms or raise alerts if any suspicious behavior is detected. Standard protection and security are also enforced in the cyber range by establishing alarms.

Video surveillance or CCTVs Closed Circuit Television – Signals are sent to a monitor in this manner so that the respective worker may notice the variation. It can aid in the observation of researchers and students for the purpose of preventing any security crimes.

Single sign-on – Access control is one of the important aspects of cybersecurity. It's all about authentication, which means that the system can only be accessed by authentic entities. The term "single sign-on" (SSO) refers to a web property that allows users to access a separate website or system. It allows users to use the same set of credentials to access several systems within a cyber-range.

Web Servers – In the cyber range, servers, machines, platforms, and workstations all work and run at the same time. The web server is in charge of processing network requests and ensuring the execution of range operations. A web server can be a piece of software, a piece of hardware, or a combination of the two that is dedicated to completing the client's requests.

Database – One of the most virtual components of the CCR is database. It is a compilation of information that allows for the addition, deletion, modification, and retrieval of data. The database contains a numerous data processing functions for performing data operations.

Management – Because so many operations are running within the CCR, it is critical to effectively control the range.

SIEM – It deals with real-time cyber range analysis and generates alarms or alerts whenever suspicious behavior is detected. Identity access control and vulnerability management are the two most important management features supported by SIEM.

Nagios – It has the ability to analyze a system, network, and infrastructure. Nagios, like SIEM, can generate alerts when a questionable behavior is detected. When the matter is resolved, it sends out a second alert. Nagios is a monitoring application that can easily monitor network services (such as FTP, HTTP, and SSH), scripts, and host resources.

Cloud – Activities and operations in a cyber-range environment, as well as real-life duplication of cyber warzone, consume a lot of resources. The Host framework in the cyber-range can be used to solve this problem.

Host-Based Antiviruses: They're required for maximizing server efficiency and availability. Furthermore, host-based antivirus takes care of server management and security issues.

Endpoint Protection Systems – These can be an app or a software program that is used to identify, control, and manage devices that seek access to the server or other services.

Firewalls – These firewalls monitor traffic entering and exiting individual devices to evaluate whether or not a packet should be allowed in. The firewall can be configured and customized according to the system requirements.

8.4. Major Features of the CyDEx Cyber-Range

There are some of the features of the Cyber-Range in question:

Cloud – Activities in a cyber-range environment and real-life duplication of cyber warzone consume a significant amount of resources. Deploying the Host framework in the cyber-range is an excellent way to overcome this limitation.

Site Metrics – the Cyber-Range is located into a high performance datacenter. The area within which the range is manufactured is defined by the site indicators framework. Despite the fact that the servers may be located in a remote location, the primary goal of announcing seats in the cyber-range is to provide access to machines and tools that will not be useful to students and researchers from outside the range.

Site Computing – relates to computer operations within the cyber-range. Because a cyber-range involves several tasks, the computers must be very capable.

Per Seat Metrics – determine the computational abilities of a single system assigned to a single seat. The exhibit area of respective computer systems in inches is 1x 34" (21:9). Any user can easily connect a laptop to the display for better quality.

Environment – In inches, the show area of the relevant computer systems is 1x 34". (21:9). Any user can easily connect a tablet to the display for improved quality.

Tools – Operating tools, intrusion detection tools, encryption tools, and some network tools are all available and used by the CyDEx Cyber-Range for security competitions, training, and testing.

Capabilities – cyber range’s capability can be described as its potential to do the job efficiently. Some of the features that contribute to the integrity of a cyber-range are listed below.

Real-World Settings – real-world risk environments and hyper-realistic environment to perform cyber defense instruction and training. It can be done by replicating network configurations, employing security tools, and simulating network site visitors.

Fully Automated – A cyber-automation range's ability ensures security, stability, and improved performance. Several components are considered operating systems, connectivity, applications & storage to swiftly produce large environments, resulting in scalability.

Controllable Testing Environment – To support the capability of the client-server system, several hosts, and configurations, the cyber range must have a manageable testing environment.

Fidelity – By employing tools in the cyber range, the cyber range ensures great fidelity. These tools could be used in a federated setting.

Reconfigurable Network Architecture – ensures that a large number of hosts can communicate. It takes into account protocol analysis, packet capture, and network monitoring.

Individual and Team Training – Individual as well as team training is available through the CCR. Individual training requires a cyber-range setting to carry out penetration testing, system defense, and capabilities that individuals may already possess.

Teams Supported – Three different teams are supported by CCR, i.e., the Red, Purple, and blue, each identified by the degree of expertise, domain, and scale.

Federation – The Cydex Cyber Range is now known for its researchers, academicians, and students' educational contributions. It is currently used for training sessions as well as multi-facility events. Because of the high-security overhead, the federated operation is not planned.

8.5 Comparison between the CyDEx Cyber-Range with Perfect Cyber Range Based On Parameters

Previously, a few parameters were considered in order to develop the ideal cyber range. Some of the most crucial parameters, as well as their significance in the ideal cyber range, have already been emphasized. Because the parameters were not quantifiable, a qualitative method of assigning values was utilized, with values ranging from Very High, Medium, High, Low, and Extremely Low. These values were given to the parameters based on their contribution and significance to the cyber range. We'll look at the same set of parameters and see how close the CyDEx cyber range is to the perfect cyber range.

Seats – The ideal cyber range assigns a medium value to the number of seats. Some cyber ranges have comparatively more seats than CCR, which has only twenty-four seats, which is a little number.

Infrastructure – For CCR, there is a robust infrastructure. Intrusion Detection Systems, Deep Packet Inspection, and firewalls all provide a variety of levels of protection and security. To ensure efficiency and performance, control mechanisms such as Supervisory Control and Data Acquisition (SCADA) and components such as balancers are used.

Scenario – The different situations that are employed to conduct functions or perform an operation are described by the cyber range scenario. Since the main goal of a cyber-range is to create a dynamic, powerful cybersecurity environment, a number of entities are working nonstop.

Tools – It is critical to provide hands-on experience in order to transmit cybersecurity skills, education, and training. If only equipment, platforms, and machines are provided, the hands-on experience will be insufficient.

People Involved – Individuals are typically hired for security administration by cyber ranges. It could be a network administrator or some technical staff who are primarily focused on assisting and assisting researchers and students in the cyber realm, and who are responsible for restoring devices in the event of any technical failures.

Simulated Environment – A replica or copy of a given environment might be described as a simulated environment. Without a simulation atmosphere, a cyber range cannot be carried out.

Automation – The state in which systems function or operate automatically is referred to as utomation. A number of cyber range components, such as control systems and intrusion detection systems, are capable of performing the functions systematically.

Performance – In the computer world, performance is defined as a system's quick response time, low resource utilization, or high resource throughput. Switches, basic routers, complicated servers, and applications are among the CCR's components.

Virtual Clone Network – In CCR, there is no Virtual Clone Network (VCN). VCN harnesses the power of a cloud platform to provide a practical cyber range zone that can be pre-configured and modified as needed.

Virtual Private Network – The ideal cyber range rates the importance of virtual private networks (VPNs) as high because VPNs can be replaced with a variety of strategies and tools.

Fidelity – The ideal cyber range must exhibit a higher level of fidelity behavior. High Fidelity Systems are well-known for providing a realistic system response during testing [35].

Cloud Infrastructure – The CCR, unlike the majority of cyber ranges, does not have a cloud infrastructure. Infrastructure deployment in the cloud is preferable to cyber-range launching in the cloud [36].

Intellectual Property – In the cyber range, a search engine or domain name might constitute intellectual property.

8.6 Representation of CyDEx Cyber-Range on the basis of parameters

The previous section details the parameters that have already been taken into account for the ideal cyber range and the CyDEx Cyber-Range. Though certain parameters have equivalent values, others are completely contradictory. In this section, we will create a graphic representation of the parameters.

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

Table 2. Importance parameters in the CyDEx Cyber-Range.

A graph can be created to illustrate the lines as parameters and the level proposed in the index, depending on the values shown in the table. To explain the same, a replacement graph is also shown.

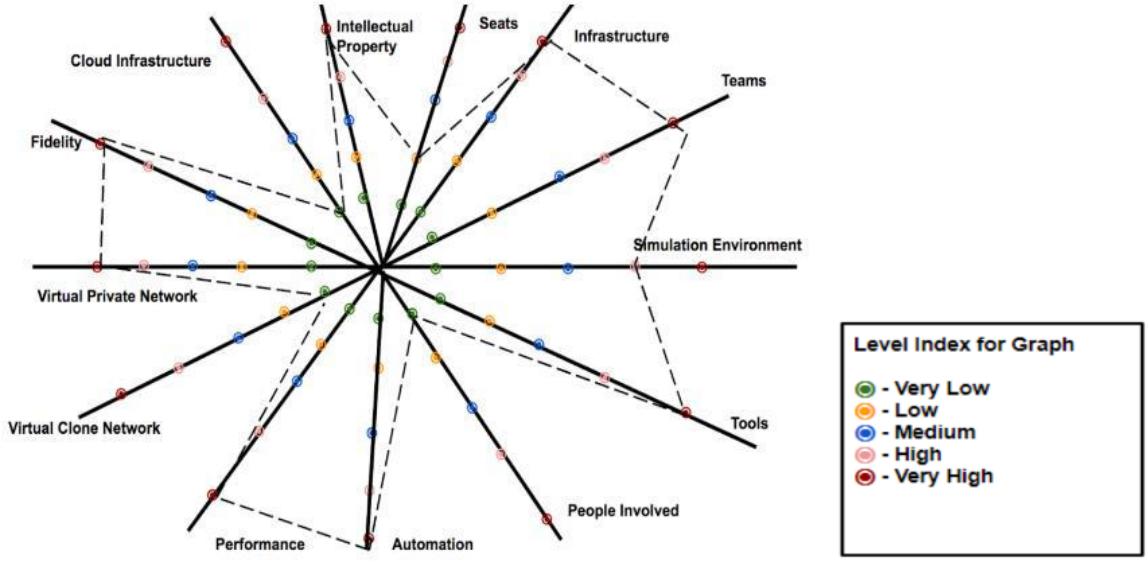

Figure 3. Illustration of the Cyber Range [37].

8.7. Qualitative study of the cydex range

We had previously planned the ideal Cyber-Range based on the Qualitative Principle attributes of the variable in consideration. Given the circumstances, we felt it was necessary to graphically illustrate the CyDEx Cyber-Range in order to follow the cyber-ranges' strong link. We will constructively apply the Qualitative Principle to establish the vicinities of the two ranges from this section.

How capable is the CyDEx Cyber-Range

We offered earlier the appropriate Cyber- range based on some various variables in the last part. We used the same variable to compare the CyDEx Cyber-Range to the ideal Cyber-Range. Despite the fact that the CyDEx Cyber-range simulates a large number of parameter values in the pursuit of the ideal Cyber-range, there are a few benchmarks that are completely different [38]. Tools, Seats, VPN, Infrastructure, Fidelity, Performance, Scenario, utomation, and Intellectual Property are parameters with the same values, whereas Simulation Environment, Cloud Infrastructure, VCN, and People Involved. The assigned values are non-quantitative, but we can calculate the quantitative value in the form of the percentage to measure the proximity of both cyber-ranges based on similar values. A given number of same parameter values divided by the total number of parameters multiplied by a hundred can be used to calculate the percentage proximity.

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

= (9/13) * 100 = appx **69.23 %**

We follow that the CCR is at least **69.23 %** the perfect Cyber-Range. The value of the cyber-range is likely to rise since it is intended to deploy Cloud Infrastructure in the future.

9. SCADA Security Concepts and Recommendations

To understand SCADA security, we must understand something about both SCADA systems and cyber security. This chapter is based on the paper **SCADA Security: Concepts and Recommendations**.

SCADA systems are the computers that control important, complex, and often dangerous physical processes, many of which constitute the physical infrastructure critical to modern societies. These physical processes are powerful tools, and their misuse generally has unacceptable consequences. Industrial control systems are old — people were controlling physical processes with dials and gauges before there were computers, and have been us in computers to assist with such control almost since the first computers were invented. As with any old field, the terminology is arcane. What the press calls a "SCADA system" is a misnomer [39].

Industrial processes can be subdivided as well. Most critical infrastructures are examples of "process industries" [40]. In process industries, the material being manipulated is more or less "goo" at some point in the physical process: water purification systems manipulate water, refineries manipulate oil, and pipelines move fluids. Electric grids are considered process industries as well, because electricity is produced in a continuous stream that can be modelled as more or less a fluid'. Even railway and traffic control systems are considered process systems, though this pushes the concept just a bit.

An important aspect common to all SCADA systems is the human operator. Control systems at important industrial facilities almost always have one or more human operators charged with ensuring the safe and reliable operation of the physical process. These operators use tools known as "human-machine interface" (HMI) software. This software almost always includes a graphical visualization of the state of the physical process, and often includes other elements such as alarm managers and historical trending tools.

This means that most often, the simplest way for an attacker to cause physical consequences is to impair the operation of some part of an operator's HMI or the systems supporting the HMI. The simplest physical consequences of such attacks are shutdowns of the physical process. Many industrial processes can be shut down much faster than they start up, and can take days to recover full production again after an emergency shutdown. In some cases, regulatory approvals must be obtained before restarting physical processes, delaying plant restarts by as much as months. Worse, emergency shutdowns can often put physical stress on industrial equipment, leading to immediate equipment failures or premature equipment aging.

9.1. Cyber Security in SCADA Systems

Cyber security is focused on preventing such attacks. SCADA security is focused on preventing any unauthorized operation of SCADA system computes. SCADA security is a more recent discipline than SCADA systems or automation systems, but is no less confusing. Newcomers to the security field see a bewildering variety of types of vulnerabilities, attacks, and defensive systems [41].

Combine this with the perennial admonition that "a chain is only as strong as its weakest link" and the task of defending controls systems can seem insurmountable. This bewildering variety is an illusion. All vulnerabilities in software and indeed in systems of hardware, software and networks, are bugs or defects. The bewildering variety is simply the result of people trying to classify somehow, all possible defects — all the possible ways people can produce software and systems incorrectly. All such classification systems are doomed to fail — people can make mistakes in an uncountable number of ways [42].

9.2. Three Laws of SCADA Security

In hopes of simplifying the field of cyber security to the point where SCADA practitioners can make sense of and routinely apply sound security practices, we propose three laws of SCADA security. Yes, in modern times, scientists prefer the terms "principle" and "theory" to "law," but we are trying to simplify things here.

1) Nothing is secure

Security is a continuum, not a binary value. Given enough time, money and talent, any security posture can be breached [39]. Anyone using terms such as "secure communications," "secure boot" or "secure operating system" is either selling something, or has just been sold a bill of goods. This is important. It changes the conversation from "never you mind, I have security covered" to "just how secure are we?" and ultimately "how secure should we really be?"

2) All software can be hacked

All software has bugs. Software development teams eliminate what bugs they can, but in spite of their best efforts, essentially all software has bugs, even security software. Some bugs result exploitable security vulnerabilities. For evidence of this, simply look at the support section of any software vendor's website and see how many security updates have been issued recently. In practice then, all software can be hacked.

3) Every piece of information can be an attack

Even a single bit of information — a one or a zero — can be an attack. If a plant operator is trying to turn off a piece of equipment with a zero, but an attacker changes that zero to a one, that is an attack. Passwords and malicious intent carried in the brains of people entering a plant can be an attack. Malware installed on brand new computers, or in the tiniest of computers embedded in USB keyboards, can be an attack.

9.3. Cyber Attacks in SCADA Systems

If IT-class protections are inadequate, then how should we be protecting SCADA systems? To address this question, we must first understand cyber-attacks. Too many SCADA security practitioners do not study modern attack techniques, and so produce singularly vulnerable "secure" SCADA systems.

Instead of attacks, too many of today's SCADA security and IT security practitioners spend far too much time thinking about vulnerabilities. Classic risk assessment calculations maintain that risk is a function of threats, vulnerabilities, exploits and consequences. Many practitioners therefore conclude that their job is to eliminate vulnerabilities. They reason that if we could only, somehow, eliminate all vulnerabilities, then our systems would be invulnerable. This chain of reasoning quickly devolves into a preoccupation with known vulnerabilities and security update programs.

The first law of cyber security states that nothing is ever secure. For example, security updates repair only known product vulnerabilities, leaving countless unknowns waiting to be discovered and exploited. More generally, SCADA systems as a whole may have vulnerabilities that stem from how the systems are organized and configured, independent of any security defects in product code [43].

These systems vulnerabilities are at the heart of many kinds of modern attacks. Frankly, our attackers are lazy — they prefer to use permissions we have configured into our SCADA networks rather than software vulnerabilities, because exploiting permissions is less work.

Corporate Insiders

Corporate insiders are people who have access to IT networks, and who are to some degree trusted by the organization. These may be employees, contractors, business partners or even third-party vendors. Insiders generally have some sort of accounts, passwords and other credentials that let them legitimately use equipment and applications on the IT network.

Corporate insiders though, tend to know little about security and less about industrial control systems. The most common targets of insider attacks are IT systems, yielding either leaked information or financial fraud.

Organized Crime

Organized crime is responsible for the vast majority of email Spam and common malware, such as viruses, worms, Trojans, botnets and ransomware. Criminal organizations pay professional malware developers to create these attack tools, and evolve these tools constantly to stay ahead of the professional anti-malware developers producing antivirus, intrusion detection and other anti-malware tools.

Organized crime has the money and talent to apply to the task of producing malware that spreads indiscriminately and infects or compromises as many machines as possible. These criminal groups typically extract an average of a few dollars value from each compromised machine. This value may take the form of stolen credit card numbers, bank account credentials, or the use of compromised computers to issue countless millions of spam messages [42].

An exception to this "low impact" rule of thumb is ransomware. **Ransomware** is malware that encrypts files and demands payment to restore the files. It is easy to imagine how encrypting files on SCADA computers could render important files unusable. This could impair the system enough to affect the operator's confidence levels, thus bringing about a safety shutdown. As ransomware becomes more pervasive, this class of common malware on SCADA networks will become a greater threat to the physical reliability of industrial systems than was the case in the past [44].

SCADA Insiders

Like IT insiders, SCADA insiders are people with access to SCADA networks and systems who are to some degree trusted by the organization.

Again, they may be employees, contractors or third-party vendors. SCADA insiders generally have some access to accounts, passwords and other credentials that let them use equipment and applications on the SCADA network. As with IT insiders, SCADA insiders tend to be well-positioned to use social engineering attacks to gain additional privileges.

Hacktivists

Hacktivists are individuals or groups with "an axe to grind" who carry out cyber-attacks. Hacktivists often have some degree of security knowledge, and can occasionally be highly skilled — they do after all spend much of their spare time hacking into other people's computers and networks. Hacktivists are amateurs though, in the sense that they generally do not profit personally from breaking into things [45].

Published reports however, indicate that no matter who the attackers were it was only hacktivist-class attack techniques and tools that were used:

- A spear-phishing campaign against employees of electric distribution systems in the Ukraine yielded remote access credentials for at least three distribution companies.
- They then logged into SCADA computers over a period of months, studying how these systems worked They Presumably also used Internet-based and other learning resources to understand how these SCADA systems were designed and configured.
- On the day of the attack, they logged in to at least three distribution companies published reports include only lower bounds on how many companies were targeted and how many people were affected. On two systems, they activated features of the SCADA software that disabled the operators' mice and keyboards and gave the attackers control of the SCADA HMI. On the third distribution system, the attackers had acquired a copy of the SCADA HMI software on their own computers. To attack this third system, the attackers used a VPN to connect their copy of the SCADA HMI to the distribution system's SCADA infrastructure.
- Over a period of about 30 minutes, the attackers used the fall software to navigate to screens for at least 30 substations and turn off power flows through those substations.

At least 200,000 people were affected for up to several hours. Concurrent with this attack, the attackers flooded the distribution companies' custom: support lines with faked phone calls. This way the targets' customers we not able to report that they had no power, which served to increase duration of the power outage.

This class of attack is known as an "Advanced Persistent Threat" (APT). APTs differ from more-widely-known, organized-crime attack in two ways:

1) The attack was most likely motivated by the Ukrainian / Russian conflict, and so had a specific target: distribution companies serving Ukrainian consumers.

2) This attack used interactive remote control — attackers were sitting at keyboards and giving commands to compromised systems for months before the 30-minute attack on substations, and for the entire duration of the 30-minute substation attack.

Note that organized crime has been known to use targeted techniques as well. Ransomware groups have started to seed modified ransomware into networks, to extort larger sums of money for decrypting an entire targeted network than could have been extorted for individual machines [46], [13].

Intelligence Agencies

State-sponsored national and regional intelligence agencies are disciplined groups of attackers using both targeted remote control techniques and when necessary, sophisticated low-volume malware. Different levels of government in China are accused of having pioneered this method of cyber espionage, and many other nations today are accused of using these same techniques [47]. At present, these attacks are used routinely to steal information about dissidents, governments, competing corporations, product designs, source code, and even designs for weapons and industrial sites [2], [48].

Many governments and authorities have expressed concern that these same attack techniques could be used to carry out sabotage rather than espionage. Some governments have declared that sabotage of critical national infrastructures will be regarded as an act of war [14].

A typical attack of this type has many steps:

1) The attackers scour social networking sites for Personal information and use spear-phishing techniques to deceive an individual in a targeted organization into clicking on an attachment or downloading a file to activate a malware payload.

2) Antivirus (AV) sensors in the targeted organization are blind to the attack, because the payload has been used sparingly. AV sensors are designed to defeat high-volume, organized-crime malware. New AV signatures are created when an AV vendor detects many thousands of copies of a new variant of malware on the vendor's Internet honeypot machines. Intelligence-agency class malware is typically deployed to a few hundred victims' sites at most.

3) The malware payload "phones home." connecting to and reporting to an Internet command and control (C&C) center. Professional operators use the C&C to connect to the malware and operate it remotely. This class of malware often has features built into it that are similar to popular "secure shell" and "remote desktop" remote access tools.

4) When the attackers steal Windows domain administrator credentials, they often create new administrator and VPN accounts for themselves, so that they no longer need to use their special malware to continue the attack.

5) When they reach their goals, they are in a position to start stealing large volumes of information, modifying information or misoperating industrial systems.

For high-value targets, the attackers may seed several kinds of malware in the target organizations, each reporting to a different control center. The least-valuable, least-sophisticated malware is used first.

Military-Grade

As I mentioned early in this thesis, nothing is secure. Military-grade attacks prove this point. Military-grade attacks not only have access to all of the attack techniques used by all of the other classes of attackers, they have enormous financial and technical resources, as well as physical attack techniques to all back on.

Military-grade attacks can physically break into targets to steal their private encryption keys and other credentials. They can intercept equipment and software on the way to customers, and insert custom hardware and malware into those shipments. Military-grade attackers can pay large sums of money for newly-discovered "zero-day" vulnerabilities in applications and cyber-security products and defenses, and can pay more money to produce custom malware to exploit and weaponize those vulnerabilities.

Transmitting Attacks

Cyber-attacks are information, and are embedded in information. Every piece of information can be an attack, even a single one/zero bit, and even information transmitted using analog signaling. What does this mean? Pretty much everyone knows that sophisticated attack code can be embedded in complex files, such as PDF files. Any communications mechanism that transmits files, including people carrying such files on removable media or cell phones in so-called "sneakernet" communications, can transmit attack code. Most people know

that any continuous stream of complex messages can encode attacks as well, such as message streams arriving across the Internet.

9.4. Failure of Defense In Depth

In response to the attacks described previously, and many other kinds of attacks, the IT approach to cyber security has been held up as the "gold standard" for SCADA security, pretty much ever since SCADA security started. SCADA security emerged as a discipline only after the World Trade Center attack in 2001, and naturally took inspiration from what was then the more mature IT security field. This tendency to take inspiration from IT security was reinforced by the IT software and hardware products that had become nearly ubiquitous in control systems by the early 2000s.

Defense in depth has failed. Modern attacks routinely compromise both IT and SCADA networks protected by IT-style defense-in-depth systems. SCADA security standards, regulations and advice are evolving beyond IT defense-in-depth, but only slowly. In spite of its clear deficiencies, many experts, and especially IT experts, still maintain that IT-style defense-in-depth is the right approach for SCADA security. It is after all, the "hammer" they know.

To understand why defense in depth has failed, we examine the IT-style approach to SCADA security in this chapter. Design-basis threat is a concept from physical security. A design-basis threat document describes the most capable adversary a site is required to defeat with a high degree of confidence. At many sites, the document is confidential or classified.

Corporate Insiders

IT-style defense in depth starts with the simplest threat – corporate insiders. The receptionist's computer in an office on another continent should not be able to send messages that confuse a control system. And so, the first defense most sites deploy is a firewall. What is a firewall exactly? A firewall is a router with a filter. What is a router? The Internet is a great many computers, routers, and the connections — wired, wireless or fiber-optic — between those computers and routers.

When the filter fails to identify an attack, the firewall forwards attack messages, generally right into the SCADA network the firewall is supposed to be protecting. In practice, there are many ways to defeat firewalls.

Defense in depth, therefore, teaches us to deploy several layers of firewalls between our SCADA systems and the Internet, each from a different vendor, and to use different kinds of communications across each layer. The reasoning here is that when vulnerabilities arc found in firewalls, communications protocols, and other systems, this design that a single vulnerability will provide an attacker reduces the likelihood with a pivoting path through the multiple layers of defenses.

Those of us who have trouble remembering our passwords on a good day are doomed if we need to remember a password to save our lives. Thus, if we are to deploy accounts and passwords on our SCADA systems, we need to pay our engineers to review or repeat some or all of their safety studies. We need to ensure that password protections are not putting people's lives at risk, or putting the reliability of the physical process at risk. Security after all, is supposed to be about enhancing safety and reliability, not impairing them.

Organized Crime

Next, IT-style defense in depth recommends deploying antivirus systems and security updates or "patches" in the language of SCADA systems. The antivirus systems should catch the majority of high-volume malware that sneaks in through the firewall and on USB drives, and the security updates should block the rest. Almost all of the high-volume malware in the world exploits known vulnerabilities and software updates eliminate such vulnerabilities.

With most plants, we have plant operators sitting in front of the SCADA system 24x7, for years at a time, because we are aiming for zero downtime. AV scanning is a real problem on our most important SCADA computers. Security updates are worse. Ask any plant engineer what it takes to bring a plant up to full capacity

after a complete refit. Take a refinery for example. Atypical refinery shuts down completely every few years for a fill' inspection, repair, and upgrade. Worn components are repaired or replaced. The SCADA group uses the opportunity to replace almost all of the computer components and upgrade software systems as much as possible, system-wide, to reflect the most recent stable versions, with the very latest security updates.

After a full month, the plant is working at 100% of capacity and everything is back to normal. *The next day Microsoft issues 73 security updates to 73 parts of the Windows operating system running on the computers at the plant.* Microsoft gives very little detail as to how much code has changed, or how the code has changed.

SCADA Insiders

Control system insiders are, again, people with legitimate physical and logical access to control system equipment. These people pose a unique threat. On the other hand, if they act to damage equipment or impair safety, it is their own health and well-being they may put at risk. Classic cyber security suggests that the best way to address this risk is with a combination of measures.

- Deploy physical access controls, to ensure that only authorized insiders have physical access to industrial equipment and control system equipment,
- Pay and treat our people well, and fairly, and so dramatically reduce the likelihood that a SCADA insider will develop malicious intent,
- Carry out personnel background checks and monitoring, to identify individuals who might be at higher-than-usual risk of becoming disgruntled or coerced,
- Set up video monitoring to provide some chance of catching physical sabotage in the act, but more to provide evidence for post-attack investigations, and
- Set up detailed cyber auditing and monitoring, again primarily to provide evidence for post-attack investigations.

In practice, SCADA insiders are the most trusted individuals in the business when it comes to the industrial equipment they operate. In practice, these detailed monitoring records can and should be used routinely to investigate safety incidents and plant shutdowns. The recordings are therefore positioned as tools to improve worker safety and uptime. Video monitoring and other audit records can be very visible in their role as tools to improve safety and reliability, and this visibility helps to deter insider attacks.

Hacktivists

By this time in our IT-style defense-in-depth design, we have built up a lot of residual risk and have only talked about compensating measures, not implemented any. At this point in the design, and to address hacktivist threats as well, IT-style defense-in-depth brings out the "big guns:" intrusion detection systems (IDSs). Given the residual risks in our defensive systems, and given the capabilities of our enemies, our IT gurus submit that compromise of our most important networks is inevitable.

Sounds convincing, doesn't it? There are serious problems with this approach

We begin with the last paragraph above. IDSs are a detective measure, not a preventive one - IDSs do not prevent compromise. A recent survey of North American energy sector executives showed that the average executive was convinced that their SCADA systems' intrusion detection systems would detect any intrusion within 24 hours of the intrusion [Error! Bookmark not defined.]. Other studies though, show that the average intrusion takes six months to detect and remediate [Error! Bookmark not defined.].

10. Case Study – SCADA Scenario (SCCR Scenario)

This chapter is based on the paper **SCADA Security: Concepts and Recommendations**.

Why include SCADA in a scenario?

- Anywhere you look in today's world, there is some type of SCADA system running behind the scenes
- SCADA systems are the backbone of modern industry

- Everything from power grids, oH and gas, traffic management systems, water treatment systems, building management systems are using SCADA
- Very complex architecture (RTUs, PLCs, relational databases, data servers, and web servers, HMIs)
- Vulnerable by design
- Usually somehow connected to the Internet (but nobody wants to admit that)
- No updates performed
- Usually black box for the personnel

SCADA Scenario is based on a Fuel Tank Monitoring System:

- Virtualised version of Guardian AST Monitoring System (SCADA System)
- Simple cleartext telnet protocol
- Very basic commands like I20100 - In tank inventory
- Internet (simulated) Connected Network
- Threat actor is APT group (Blueweeder)

Enemy rational: Disrupt mission directly and cause political dilemmas inside the troop contributing nations by causing fear with the population

To fulfil its goals, a group of hackers from Stellaria[1] attacks a SCADA system in order to disrupt Tytan's main military airbase located in Lastopol (in Tytan), which is also housing MATO medical evacuation, tactical and reconnaissance aircraft jets, as well as troops that are supporting a local mission. Similar attacks against SCADA systems are planned against troop contributing nations.

10.1. Scenario Calendar - Sequence of events:

1 month before STARTEX

- Blueweeder has identified a zero day vulnerability affecting a very popular fuel control SCADA system used by MATO nations, and in support of the MATO mission in Tytan
- The attackers have managed to get access to various national networks (not in mission) which are using the vulnerable SCADA system, and have placed a logic bomb in the HMI (human - machine interface). The logic bomb will be activated automatically (without requiring further interaction) on STARTEX+1
- The logic bomb when activated, interferes with the volume measuring system and presents to the operators 30% less volume than the actual volume in the tanks

6 days before STARTEX

- Blueweeder gains access to the SCADA system in Lastopol airbase. They infect the system with the logic bomb which is activated later on the same day.

5 days before STARTEX

- Explosion in Lastopol airbase, caused by overfilling of the fuel tanks. Two local workers (Tytan nationals) are killed. Air operations are affected as aircrafts cannot be refueled. As a result the airbase is nonoperational for at least 7 days.

4 days before STARTEX

- Tytan's officials after initial investigation suspect a cyber attack and request RRT support from MATO
- Tytan releases information related to the type of SCADA system that was attacked to all troop contributing nations. Nations begin a national inquiry to identify national usage of this type of SCADA

STARTEX (day 1)

- RRT arrives in Lastopol air base and starts investigating under the direction of MATO's CERT

- Blueweeder takes responsibility for the attack. It demands that nations stop supporting the operation and recall their military forces within 48 hours, otherwise similar attacks will take place in their capitals
- Nations begin to investigate similar SCADA systems based on ttie identified national usage resulting from the recent inquiry

STARTEX Day 2

- Logic bomb is activated in the national SCADA systems
- Wrong values are presented to the monitoring interface and fuel tanks contain more fuel than what is actually reported to the operators

STARTEX Day 3

- As nations haven't recalled their military forces, and overfilling of the tanks can take from hours to days, Blueweeder tries to connect to the SCADA systems and further change the values to cause tanks to overfill more quickly
- If Blueweeder succeeds (players has not removed the logic bomb and has not identified how the attackers gained access to the network), the tanks will explode at 13:00 Zulu
- If Blueweeder doesn't manage to gain again access but the logic bomb is still active, the tanks will explode at 15:00 Zulu
- Explosion is simulated by shutting down the SCADA VM

10.2. National Segment Architecture & Attack path

There are 29 network segments (Countries) for which you will have to simulate the attack steps. Thus, you will need to repeat this section 29 times. The easiest solution is to get X segments each and work in parallel. As an attacking path, Blueweeder (the bad guys) will compromise multiple fuel control SCADA systems in nations, and infect them with a logic bomb that will interfere with the volume measuring system. This will cause the fuel tanks to overfill and explode. They have identified that a vulnerable VNC Server (the version of the VNC is vulnerable to authentication bypass) is running on their targeted infrastructure. By exploiting this service they gain access to a system on the LAN (VM1) with local admin privileges.

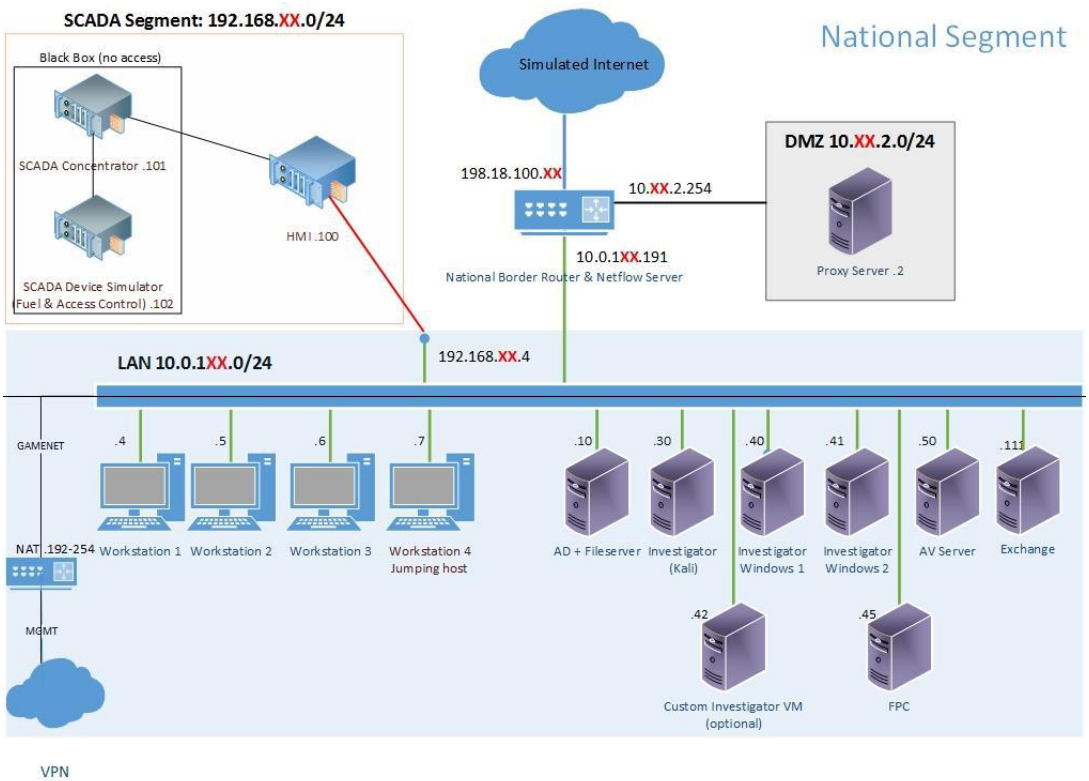

Figure 4. Network Architecture of each segment.

They use mimikatz to dump cached credentials from memory, and as a domain admin has connected to this workstation previously, they gain domain admin rights. Then they enumerate the LAN and identify that there is a VM which has two network interfaces. This VM allows them to access the SCADA segment. They RDP to it, scan the SCADA segment and identify the SCADA systems and HMI (admin interface).

They exploit an SQL injection vulnerability on the HMI, gain access to the server and install the logic bomb (PHP code on the web interface). For network monitoring there is a sollution called nfsen, used for network statistics for internal connections (between LAN VMs) and also to/from the Internet and two Windows VMs and a Linux (kali) investigator VM provided for investigation.

Potential Solution

- Connection from a Stellarian IP to the (netflow)
- Proxy logs with the tools that attacker's have downloaded on internal systems (border router acts as a proxy server)
- Connections from compromised workstation to all internal systems (netflow) during info gathering
- Windows event logs (authentication)
- Web server logs on HMI (no access to the SCADA VM)

Training objectives covered

The SCADA cyber incidents affects the MATO mission directly and indirectly (threatening troop contributing nations in their own country). National training audiences should consider reporting lines to national and MATO strategic stakeholders. Stakeholders can be either training audiences or role-players to exercise impact analysis and reporting. The SCADA exercise environment requires analysis of: netflow traffic, proxy logs, event logs and OS forensics, to identify and resolve the vulnerability of the SCADA system. Technical findings of the SCADA analysis need to be administered and reported in line with national/MATO procedures. Findings need to be shared with all relevant national/MATO stakeholders following the applicable reporting lines.

11. Identification & Analysis of a Fileless Malware in a Cyber Range

Numerous organizations think that utilizing well-known antiviral solutions helps to protect their endpoints from all types of attacks. A weekly scan and rapid signature update are only as good as the threats it knows how to detect. Antivirus companies' prevention mechanisms are based on a variety of methods, including heuristics (what the file does), signatures (a copy of the file), and other indicators (reputation, DNS or registry changes, and so on.) People also utilize firewalls to avoid downloading, malicious code execution, and malware exfiltration, in the hopes of preventing unexpected behavior when running scripts or files containing malware.

11.1. What is a fileless malware?

Protecting yourself entails more than just upgrading your AV and running scans on a regular basis, and there are a few main challenges in dealing with fileless attacks using only traditional AV and Firewalls:

- Fileless attacks do not create a file, rendering file-based detection methods obsolete.
- Fileless attacks are used in targeted attacks and as the first stage of malware infection using a browser, but full attacks are now fileless.
- Attacks without a file often pivot from memory exploits to PowerShell code that most endpoint solutions don't inspect. These white-listed apps have complete control to replicate and remove fileless components, as well as move to legitimate access.
- Patch processes aren't quick enough to keep up with browser patches or app patches.
- Many AV endpoint solutions claim to protect against memory exploits and scripts, but most are vague on the details making it hard for buyers to compare solutions.

In a few words, PowerShell is:

- Microsoft introduced the PowerShell framework in 2005
- Offers a scripting language and command-line shell, ideally for automating and managing tasks
- Because of it's power, it was also quickly adopted by attackers

PowerShell is also a great attack platform :

- Mainly used as a downloader and for lateral movement
- Easy to obfuscate PowerShell code
- Hard to analyze obfuscated code
- AVs static signatures are inefficient on obfuscated code
- Often overlooked by traditional security products and defenders when hardening their systems
- It has a growing community with ready available scripts

11.2. Detection and prevention of fileless malware

What makes detecting fileless malware attacks so difficult? These attacks are completely completely in memory, and they use legitimate system administration tools to execute and propagate, making identifying what is legitimate PowerShell usage and what is attacker activity extremely difficult. PowerShell is used by IT administrators to do a variety of tasks on a daily basis, hence a large amount of PowerShell is required.

IT administrators use PowerShell to do a variety of tasks on a daily basis, thus a large amount of PowerShell usage shouldn't cause concern. And because PowerShell is so widely used, security professionals lack the time to study logs, identify suspicious behavior, and investigate the occurrence.

Disabling PowerShell is a common misconception that will prevent fileless malware attacks. Regrettably, this approach will just make IT professional jobs more difficult. PowerShell is only necessary to carry out the most basic functions. In addition, PowerShell will eventually be used by all Microsoft products.

Administrators who become proficient in PowerShell will be able to manage the majority of Microsoft's newest products. The use of PowerShell is restricted, limiting administrators' abilities to honed talents that could aid their careers.

11.3. Case Study – Fileless Malware Scenario (FMW Scenario)

Storyline summary

Blueweeder targets Governmental networks involved in the design, testing and deployment of NATO's Air Defence System (ADS) in Tytan.

Objective

- Slow down the project by causing data loss
- Even unclassified data (e.g. shipping schedule, Delivery POC etc. can be useful for Stellaria!)
- Gain INTEL on the air defense system (secondary) Impact

Technical challenges

- Computer forensics
- Network forensics
- Malware analysis

Scenario Calendar - Sequence of events

3 weeks before STARTEX

– Blueweeder starts sending spear phishing emails
– Infects multiple workstations in Nations with malware, which remains dormant

1 day before STARTEX

– Malware activates. Exfiltrates & deletes files slowly
– Users start complaining that some of their files are missing

STARTEX

– Technical teams begin investigation

National Segment Architecture & Attack path

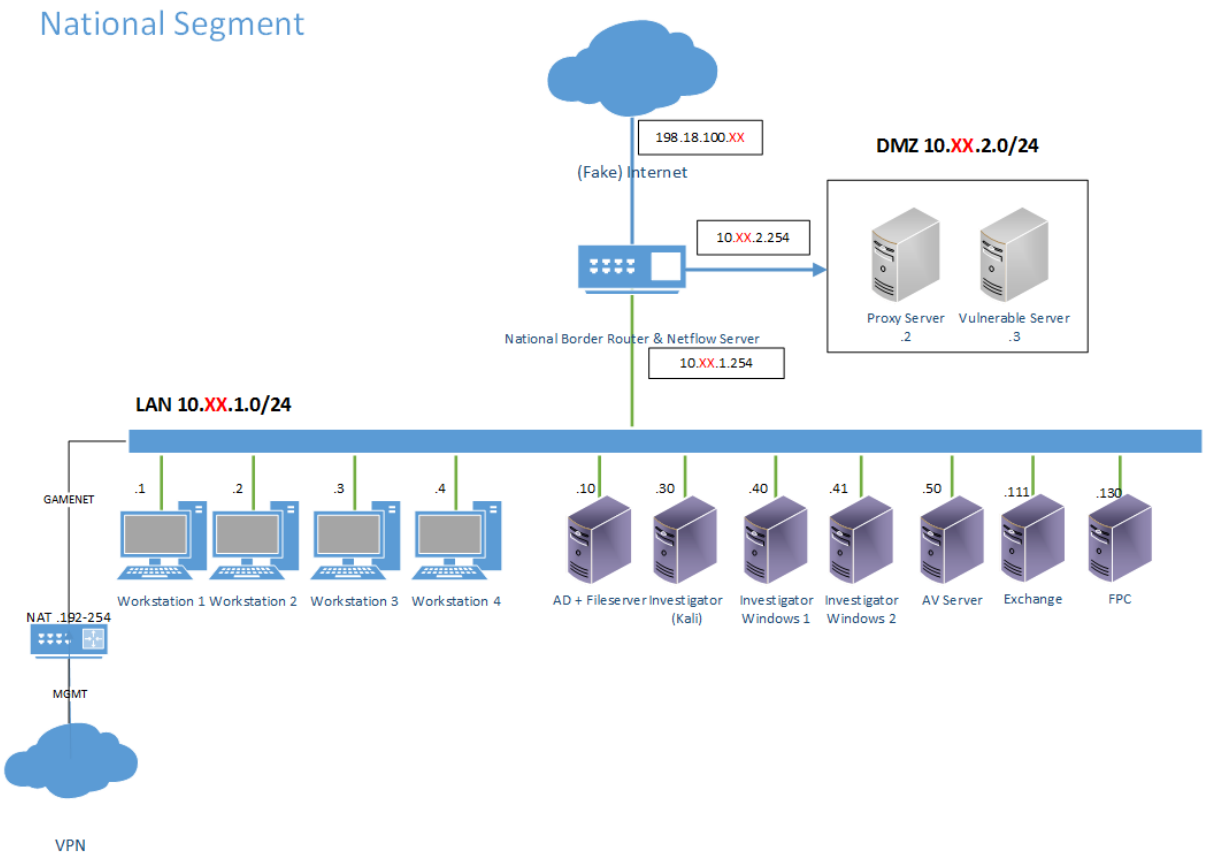

Figure 5. Diagram of a National Segment.

Initial infection

Spear-phishing attack against 2 users per Nation. Email with Word (or other macro-enabled) document The document will contain a small **powershell script (Stage 1)** encoded in the macros Stage 1 will be dropped in the AppData directory and a scheduled task will be added to execute it every 2 hours, starting from STARTEX – 1

Stage 1

Each time it is executed it will:

– Get the domain name
– Do 3 GET Requests to BadIP (Blueweeder)
  • URL will be used as a key (like port knocking).
  • This will enable a firewall rule on BadIP to allow connections from that IP (gateway IP)
– Do a HTTP request to BadIP port 80/TCP sending the domain name
  • BadIP will return the Stage 2 powershellscript which will be executed in memory
– Unique for each nation

– Connects to a C&C server in a different country

Stage 2

The actions performed by Stage 2 are:

– Search on local hard drives and mapped network drives for MS office and PDF files, and select randomly 5

– Generate a random key (256 bit)

– Send the filenames, hashes of the encrypted files and the encryption key to the C&C, encrypted with the public key of the C&C

– Encrypts (AES 256) the 5 files, sends them to the C&C server, & deletes them – Exits (will start again at the scheduled interval)

Expected milestones during execution

- Find initial infection
- Identify infected workstations & malicious process (Stage 1)
- Perform malware analysis on Stage 1&2
- Collaborate with the nation where your files are uploaded to (get encrypted files, key)
- Share your findings

12. Conclusion and future directions

12.1. Conclusion

In this thesis we have analyzed several cyber ranges and their types. Because now we can say that know that different cyber ranges have distinct strengths and weaknesses, we create an Ideal Cyber Range using classification parameters. Various tables and figures have been used to represent classifications. We assign a level of importance to each parameter based on its significance.

Further, we have introduced the Next-Generation Cyber Range. The range is accountable for initiating several cybersecurity scenarios, which have also been recognized, as a cybersecurity training and awareness center.

As a part of the functionalities and architecture a SCADA scenario has been developed and run with 30 teams (red team and blue team).

Another important scenario that can put in value the characteristics and functionalities of a next generation cyber range and can improve awareness in any type of cybersecurity team (red, blue, purple) is the fileless malware scenario presented in the thesis.

12.2. Main contributions

I was involved in the process of research and development of various cyber-ranges and those can be considered a strong result of this thesis. I evaluated current cyber-ranges and categorized them based on certain factors as part of the survey, as I observe that different cyber-ranges have different strengths and limitations.

Using the categorization parameters, I presented a perfect Cyber-Range. To represent the clasification, several tables and figures have been utilized. I assigned a level of priority to each parameter based on its outcome. The accompanying graphs provide a good picture of what parameters must be considered for a Perfect Cyber-Range.

An important part of this research was the design and deployed of the cyber range for NATO Cyber Coalition exercise (2015-2018) based on Estonian MoD infrastructure. In order to create a good proof of concept I was also involved in the development of the SCADA scenario for NATO Cyber Coalition 2017 exercise where I was able to simulate a critical environment that might be attacked by malicious actors.

I was also involved in the scenario development and infrastructure deployment for NATO Cyber Coalition 2018 exercise that was based on a Fileless Malware Scenario. In Romania I was part of the team that organised

(deployment of the exercise infrastructure and scenario contribution) the CyDEx Exercises in 2017 and 2018 and in 2019 I was part of the Deloitte team that created the red team scenario and played that scenario in real-time during the CyDEx 19 exercise.

We can conclude that the main contributions of the research for this thesis are:

- We studied complex architectures and features that can be used in cyber ranges and compared three of the most important existing cyber ranges - between US Cyber Test Range, NATO Cyber Range (CCD COE Cyber Range) and UK Cyber Range. The results are presented in Chapter 2;
- We identified the most used architectures and characteristics in world wide cyber ranges and described various topologies that might be implemented in different types of red team-blue team scenarios. The results are presented in chapters 5 and 6;
- We identified the key aspects of a next generation cyber range and described the essential parameters that can define the perfect cyber range (seats, infrastructure, scenario, staff involved, simulated environment, tools, automation, performance, VPC, VPN, fidelity and intelectual property). All those parameters were highlighted on Cyber Range from the CyDEx Annual Exercise. We also made a comparison between CyDEx cyber range and the perfect cyber range concept. The results are presented in chapters 7 and 8;
- We identified the advantages in increasing awareness for cyber security departments and critical infrastructure such as SCADA systems. Also identified the main security concepts and concerns on SCADA systems, the attacking vectors and the defence perspective. All of the results are presented in chapter 9;
- We proposed practical scenarios for critical cyber security infrastructures that were developed in real-world cyber exercises, on NATO Cyber Coaliton and CyDEx. The scenarios include attacking vectors, investigation steps for analysis and recommendations to protect against this kind of attacks that were presented in detail in chapters 10 and 11.

12.3. List of Publications

1. **Dragos-George Ionica**, Florin Pop and Aniello Castiglione - ***Creating and Managing Realism in the Next-Generation Cyber Range***. Published in Network and System Security12th International Conference, NSS 2018, Hong Kong, China, August 27-29, 2018,
2. **Dragos-George Ionica**, Nirvana Popescu, Decebal Popescu, Ciprian Dobre - ***SCADA Security: Concepts and Recommendations***: 10th International Symposium, CSS 2018, Amalfi, Italy, October 29–31, 2018
3. **Dragos-George Ionica**, Nirvana Popescu, Decebal Popescu, Florin Pop - ***Cyber Defence Capabilities in Complex Networks*** - INTERNET OF EVERYTHING - ALGORITHMS, METHODOLOGIES, TECHNOLOGIES AND PERSPECTIVES 2018
4. Andrei Stoicu, **Dragos-George Ionica** - ***Social Media Avatar: My Dear Virtual Assistant***. Published in: 2018 IEEE 16th International Conference on Embedded and Ubiquitous Computing (EUC)
5. Marius Marian, Adelin Cusman, Dan Popescu, **Dragos Ionica** - ***A DNP3-based SCADA Architecture Supporting Electronic Signatures***. Published in: 2019 20th International Carpathian Control Conference (ICCC)
6. Marius Marian, Adelin Cusman, Florin Stinga, Dan Popescu, ***Dragos Ionica*** - ***Experimenting with Digital Signatures over a DNP3 Protocol in a Multitenant Cloud-Based SCADA Architecture*****.** Published in: August 2020 IEEE Access PP(99):1-1

12.4. Other activities

- Participation at BlackHat USA and DefCon conferences in 2017
- Participation at Offensive Con 2019 & 2020
- Red Team Operator (Certification issued by Zero Point Security) in 2020
- Adversary Tactics: Red Team Operations (Certification issued by Specter Ops)
- Part of the COE Cybercrime Program

- Top 5 Cobalt Core Pentesters of 2020 on Cobalt PaaS platform https://blog.cobalt.io/exploring-valuable-pentester-traits-top-cobalt-core-pentesters-of-2020-e8d1fc0389ae

12.5. Feature directions

I was effective in classifying cyber-ranges into several categories based on my research. There are many more cyber-ranges that work in a variety of ways, increasing the potential for more such parameters in the future. The level of importance assigned to each parameter for a ideal cyber- range may vary accordingly, based on the analysis of several other cyber- ranges. The assessment can only be made on the basis of logic and conviction because the data collected is not quantitative. In the future, I can learn more about how cyber-ranges work and collect data for a variety of cyber-ranges in order to provide quantitative data to a perfect cyber-range.

It has been revealed that the Next Generation Cyber-Range is very comparable to the Perfect Cyber-Range when used in a real-world context. Several parameters, such as Cloud Infrastructure, Simulation, People Involved, and Virtual Clone Network (VCN), have different values, resulting in discrepancies. While cloud infrastructure is being deployed, sophisticated tools may be used to improve simulation, and people may be incorporated in the future, parameters like VCN may not be part of the cyber-range anytime soon. As a result, the percentage proximity between the cyber-ranges could significantly grow. New parameters can also be added to the analysis.

References

[1] "Defence Minister opens UK cyber security test range - GOV.UK," [Online]. Available: https://www.gov.uk/government/news/defence-minister-opens-uk-cyber-security-test-range. [Accessed January 2021].

[2] N. Wiener, Cybernetics or Control and Communication in the Animal and the Machine, Cambridge: MIT Press, 1948.

[3] "NATO Cooperative Cyber Defence Centre of Excellence. CCD COE Training Courses -CCD COE.," [Online]. Available: https://ccdcoe.org/training/. [Accessed July 2020].

[4] M. . J. West-Brown , D. Stikvoort , K.-P. Kossakowski , G. Killcrece, R. Ruefle and M. Zajicek , "Handbook for Computer Security Incident Response Teams (CSIRTs)," Software Engineering Institute, April 2003.

[5] NC3A, "Cyber Defence Capability Framework," December 2010.

[6] P. A. Bauxbaum, "Building a Better 'Cyber Range'," August 2011.

[7] E. Powell, "The Information Assurance Range," *ITEA Journal,* vol. 31, pp. 473-477, 2010.

[8] Welshans, "History of Cyber Testing and Evaluation - A Voice From the Front Lines," *ITEA Journal,* vol. 31, pp. 449-452, 2010.

[9] UK Ministry of Defence, "Defence Minister opens UK cyber security test range.," [Online]. Available: http://www.mod.uk/DefenceInternet/DefenceNews/DefencePolicyAndBusiness/Defence Minister OpensUkCyberSecurityTestRange.htm.

[10] J. e. a. Mirkovic, "The DETER Project; Advancing the Science of Cyber Security Experimentation and Test," *IEEE,* 2010.

[11] "DARPA. National Cyber Range. DARPA. 21. Defense Information Systems Agency. Department of Defense Information Assurance Range: A Venue for Test and Evaluation In Cyberspace.," [Online]. Available: http://www.darpa.mil/Our_Work/STO/Programs/National_Cyber_Range_(NCR).aspx. [Accessed August 2011].

[12] W. e. a. He, "A game theoretical attack-defense model oriented to network security risk assessment," *Computer Science and Software Engineering,* 2008.

[13] R. a. L. P. Ottis, "Cyberspace: Definitions and Implications," in *5th International Conference on Information Warfare and Security*, Dayton OH, US, 2010.

[14] D. D. S. H. S. a. L. K. W. F. D. K. Kuehl, " Cyberpower and National Security," in *From Cyberspace to Cyberpower: Defining the Problem.*, 2009.

[15] Ministry of Security and Justice, "Cyber Security Beeld Nederland," June 2012. CSBN-2. .

[16] D. L. D. C. a. C. Y. Paul Cornish, "On Cyber Warfare," *Chatham House,* November 2010.

[17] Ginter, "13 ways through a firewall: What you don't know can hurt you. ISA Intech," 2013. [Online]. Available: https://www.isa.org/standards-publications/isa-publications/intech-magazine/2013/april/special-section-13-ways-through-firewall-what-you-dont-know-can-hurt-you/ .

[18] US Department of Defence, "Joint Publication 3-0, Joint Operations.," August 2011.

[19] E. Ferrara, " Determine the business value of an effective security program - information security economics 101," *Forrester Research,* 2002.

[20] A. W. B. Conklin, "E-Government and Cyber Security: The Role of Cyber Security Exercises," in *39th Hawaii International Conference on Systems Sciences*, 2006.

[21] The White House, "International Strategy for Cyberspace," 2011. [Online]. Available: http://bruteforcelab.com/wp-content/uploads/HILJ-Online_54_Schmitt.pdf.

[22] NATO, "Allied Joint Doctrine for Information Operations," vol. AJP 3.10, November 2009.

[23] J. D. a. S. Magrath, "A survey of Cyber Ranges and Testbeds," *Cyber and Electronic Warfare Division Defence Science and Technology Organisation, Australian Government Department of Defence,* 2013.

[24] "Enisa - European Network and Information Security Agency," *Good Practice Guide on National Exercises,* 2009.

[25] D. A. S. Sr, "'Communications-Electronics Command cyber training range launches', Logistics and Readiness Center, CECOM," 23 June 2015. [Online]. Available: https://www.army.mil/article/150996/communications_electronics_command_cyber_t.

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

[27] "The Role of Local Law Enforcement Agencies In Preventing and Investigating," April 2014.

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

[29] "Image for Cisco Cyber Range," [Online]. Available: http://www.manetic.org/images/stories/events/20170424/20170424.JPG .

[30] Cyberbit, "Cybershield Training and Simulation, Live training for cyber-security professionals," 2016. [Online]. Available: https://www.cyberbit.com/wpcontent/uploads/2016/09/CB-TnS-Print.pdf.

[31] M. Gürtler, "'NATO Cooperative Cyber Defence Centre of Excellence', Locked Shields," 27 June 2012. [Online]. Available: https://www.enisa.europa.eu/events/cyber-exercise-conference/presentations/7.%20Conf%20Paris%20-June%202012%20-%20-%20M.%20GURTLER%20-NATO-CCDCOE.pdf .

[32] Department of Defense, "National Cyber Range, Test resource Management Center," 24 February 2015. [Online]. Available: https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf.

[33] "Baltimore Cyber Range (About), August 2017," [Online]. Available: https://www.baltimorecyberange.com/about .

[34] E. Tate Emily, "Regent University opens stand-alone cyber range," Regent Cyber Range, October 2017. [Online]. Available: https://edscoop.com/regent-university-opens-stand-alone-cyber-range.

[35] J. Curry, "CyberSecurity Range (CSR) v2.0 Architecture and Capability," Defense Information Systems Agency (DISA), April 2016. [Online]. Available: http://www.disa.mil/~/media/Files/DISA/News/Conference/2016/AFCEASymposium/5-Curry20Improving_Cyber_Security.pdf.

[36] " Georgia Cyber Range," [Online]. Available: http://cyber.augusta.edu/au/wp-content/uploads/2017/01/videobgtest.png.

[37] "Image for NATO cyber range," [Online]. Available: https://www.nato.int/nato_static_fl2014/assets/pictures/stock_2017/20170406_170406.

[38] R. C. Range. [Online]. Available: https://www.raytheon.com/index.php/cyber/news/feature/ready-aim-test.

[39] Ponemon Institute, "2016 Ponemon Cost of Data Breach Study," Ponemon Institute, 2017. [Online]. Available: https://www.ibm.com/security/data-breach/.

[40] Tripwire, "Tripwire Critical Infrastructure Study," 2015. [Online]. Available: Available: https://www.tripwire.com/company/press-releases/2015/01/study-critical-infrastructure-executives-complacent-about-internet-of-things-secu/. [Accessed January 2017].

[41] "The Georgia Cyber Range," [Online]. Available: https://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/press_release/Georgia%20Cyber%20Innovation%20and%20Training%20Center.pdf.

[42] CBC News, "University of Calgary paid $20K in ransomware attack," 2016. [Online]. Available: http://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979.

[43] Mandiant, "Mandiant APT1 – Exposing One of China's Cyber Espionage Units," 2013. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[44] S.Gallagher, "Two more healthcare networks caught up in outbreak of hospital ransomware," Arstechnica, 2016. [Online]. Available: https://arstechnica.com/security/2016/03/two-more-healthcare-networks-caught-up-in-outbreak-of-hospital-ransomware/.

[45] R. Eller, "Black Hat Japan 2004 - capture the flag games/ measuring skill with hacking contests," 15 October 2004. [Online]. Available: http://www.blackhat.com/presentations/bh-asia-04/bh-jp-04-pdfs/bh-jp-04- eller/bh-jp-04-eller.pdf. [Accessed July 2018].

[46] M. o. Defence., "Ministry of Defence. Defense after the credit crisis: a smaller armed forces in a troubled world," BS2011011591, 2011.

[47] Mandiant, "Mandiant APT1 – Exposing One of China's Cyber Espionage Units," 2013. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[48] T. Scott, "March 17 1948: William Gibson , Father of Cyberspace," [Online]. Available: Wired.com. [Accessed March 2011].