# EFFECTS OF A DDoS ATTACK ON A MILITARY OPERATION

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF INFORMATICS OF
THE MIDDLE EAST TECHNICAL UNIVERSITY
BY

LÜTFİ KILIÇ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF INFORMATION SYSTEMS

MARCH 2018

Approval of the thesis:

**EFFECTS OF A DDoS ATTACK ON A MILITARY OPERATION**

Submitted by Lütfi KILIÇ in partial fulfillment of the requirements for the degree of **Master of Science in the Department of Information Systems, Middle East Technical University** by,

Prof. Dr. Deniz ZEYREK BOZŞAHİN
Dean, **Graduate School of Informatics** ____________________

Prof. Dr.Yasemin YARDIMCI ÇETİN
Head of Department, **Information Systems Dept.** ____________________

Assist. Prof. Dr. Cengiz ACARTÜRK
Supervisor, **Cognitive Science Dept.** ____________________

**Examining Committee Members:**

Assoc. Prof. Dr. Tuğba TAŞKAYA TEMİZEL ____________________
Information Systems Dept., METU

Assist. Prof. Dr. Cengiz ACARTÜRK
Cyber Security Dept., METU ____________________

Assist. Prof. Dr. Aybar Can ACAR
Helath Informatics Dept., METU ____________________

Assoc. Prof. Dr. Aysu Betin CAN
Information Systems Dept., METU ____________________

Assist. Prof. Dr. Özkan KILIÇ ____________________
Computer Engineering Dept., Yıldırım Beyazıt University

**Date:**

**I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.**

**Name, Last name : Lütfi KILIÇ**

**Signature :**

# ABSTRACT

## EFFECTS OF A DDoS ATTACK ON A MILITARY OPERATION

KILIÇ, Lütfi
MSc., Department of Information Systems
Supervisor: Assist. Prof. Dr. Cengiz ACARTÜRK

March 2018, 61 pages

Abstract: The goal of the present study is to investigate the underlying mechanics of a likely interaction between two phenomena, namely “War” and “DDoS Attacks”, using computational methods. For this, first, we study the characteristics of the Lanchester Combat (Kinetic) Model, the Kermack and McKendrick’s Epidemic (S-I-R) Model and the Mixed Epidemic Model. Then we propose a computational model and run simulations that simulate the influence of DDoS on the available combat model. The analyses and the results of simulated data reveal the potential influence of DDoS attacks, by providing insights about the cyber war effects on war and casualties that may impact the fighting sides.

Keywords: Lanchester Combat (Kinetic) Model, Epidemic Model (S-I-R), Mixed Epidemic Model, Cyber War, DDoS Distributed Denial of Service Attack.

# ÖZ

DDoS ATAKLARININ ASKERİ OPERASYONLARA ETKİLERİ

KILIÇ, Lütfi
Yüksek Lisans, Bilişim Sistemleri Bölümü
Tez Yöneticisi: Doç. Dr. Cengiz ACARTÜRK

Mart 2018, 61 sayfa

Bu çalışmanın amacı iki fenomen kavram, "Savaş" ve "DDoS Saldırısı" (Dağıtık Servis Engelleme Saldırısı) arasındaki olası etkileşimin mekanik altyapısını hesaplamalı modeller yoluyla araştırmaktır. Bu amaçla öncelikle, Lanchester Combat (Kinetic) Modeli, Kermack ve McKendrick's Epidemic (S-I-R) Modeli ve Mixed Epidemic Model'in karakteristikleri incelenmiştir. Daha sonra hesaplamalı bir model öne sürülmüş ve DDoS saldırısının mevcut savaş modeli üzerine etkisini gösteren simülasyonlar çalıştırılmıştır. Analizler ve simülasyon verisi sonuçları DDoS saldırılarının savaştaki taraflar üzerindeki potansiyel etkilerini ortaya çıkarmıştır.

Anahtar Sözcükler: Lanchester Combat (Kinetic) Modeli, Eidemic Model (S-I-R), Mixed Epidemic Model, Siber Savaş, DDoS Dağıtık Servis Engelleme Saldırısı.

I dedicate this study to my wife, Elçin and my daughters, Rana and Sena who were born during my education in the Middle East Technical University. Without my wife's continuous support and unconditional love, it would be too difficult to overcome the hard work required for this study.

Our daughters, Rana and Sena, have brought spring to our life and their smiling faces gave me encouragement and motivation to handle the workload at my studies. I am grateful to have such a wonderful family.

# ACKNOWLEDGMENTS

First and foremost, I would like to thank my advisor Asst. Prof. Dr. Cengiz ACARTÜRK for honoring me by accepting as his student and opening the way for my education at the Middle East Technical University. I am grateful for his support and dedication he has constantly provided for me during this study.

I would like to thank my committee members, Assist. Prof. Dr. Aybar Can ACAR, Assist. Prof. Dr. Cengiz ACARTÜRK, Assoc. Prof. Dr. Aysu Betin CAN, Assoc. Prof. Dr. Tuğba TAŞKAYA TEMİZEL and Assist. Prof. Dr. Özkan KILIÇ for their technical guidance, encouragement and support during my course of thesis study.

I would also like to sincerely thank Informatics Department's faculty members and staff for their help. As a researcher out of the field, I never felt alone and my teachers always helped me to feel more comfortable and understand more in classes.

Finally, I want to thank graduate students of Informatics Department. They never left me alone and accepted me as their friend. I am truly grateful of their friendship and hospitality.

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF GRAPHICS

# LIST OF ABBREVIATIONS

| | |
|---|---|
| **ADDoS** | Anti-DDoS |
| **AER** | Attack Efficency Rate |
| **DDoS** | Distributed Denial of Service |
| **IRR** | Infection Remove Rate |
| **ISR** | Infection Spread Rate |
| **KARB** | Kinetic Attack Rate of Blue |
| **KARR** | Kinetic Attack Rate of Red |
| **ODE** | Ordinary Differential Equation |
| **ADS** | Anomaly Detection System |

# CHAPTER 1

# INTRODUCTION

## 1.1. Purpose and Scope

The purpose of this study is to investigate the underlying mechanisms of the interaction of two phenomena: “War” and “DDoS Attacks”, by using computational methods. We employ analytical and computational methods to reach this goal. Accordingly, the scope of this thesis is twofold: to propose an analytical framework that addresses the relationship between War and DDoS attacks and to  propose a model that can be verified by computational analysis. In particular, battlefield modelling was done by applying the Lanchester Combat Models and incorporating DDoS attacks into the model. In DDoS modelling we employed the Mixed Epidemic Model as presented in the following chapters.

## 1.2. Thesis Organization

This thesis is organized as follows. Chapter 1 defines the purpose and scope of the study. The second chapter introduces the concept of “war” from a scientific perspective, the concept of “cyber”, and the relationship between the two concepts. The third chapter defines the differential equations that were employed to implement the interaction model. The fourth chapter presents the proposed model itself. The data generated with simulation are also presented and commented in Chapter 4. The final chapter concludes the thesis by discussing the findings and addressing future work.

## 1.3. Research Question

There exist models on warfare and cyberwarfare in the research literature. However, there is no specific model that directly addresses the effects of a DDoS attack on a military operation. The research question of the present study is to explore the associations between a DDoS attack and a military operation and consequents thereof.

## 1.4. Research Method

To develop the model, the relationship between a DDoS attack and a military operation[1] was defined by five variable factors in a mathematical model, and the model was run by a simulation. A base case was set for the control group, and at, each time, a single factor was updated to interpret the effect of the factor in comparison to its base values, as described in Chapter 4. The following chapter presents the background terminology for the proposed model.

[1] The terms "war" and "military operation" are used interchangeably in this thesis.

# CHAPTER 2

# BACKGROUND TERMINOLOGY

## 2.1. Introduction

This thesis is about modelling the battlefield. Therefore, in this chapter, we present how technology influences the military forces, as well as its consequences on the battlefield. Additionally, the terms “war”, “cyber” and “cyber warfare” are introduced.

Information technologies have influence upon financial systems, industrial services, government bureaucracy, public utilities, organizational services, manufacturing processes and military conducts worldwide (Lindsay, 2013). In particular, the Internet has become increasingly crucial to modern societies. It has been changing the way we communicate, make business and act in our everyday life. Digital systems control many vital aspects of the modern society, from basic financial services to transportation systems. These services have technical vulnerabilities. Therefore, our dependence on these systems is a crucial factor that renders cyber war inevitable.

The term “cyber” has been increasing its active role in multiple aspects of societal life. The term was first used by Norbert Wiener (Wiener, 1948). According to the Merriam-Webster Dictionary, cyber is defined as “of, relating to, or involving computers or computer networks.” In a “cyber” environment, valuable information assets are usual targets that can be exploited by the attackers. Even ordinary actors, such as end-users, or the two sides in a military operation may create major asymmetric impacts (McGraw, 2013). The asymmetrical side of cyber has paved the way for military conducts of networks to deter the enemies.

The use of cyber to gain sensitive data, thus accomplish military objectives introduced the concept of “cyber warfare”. There are various definitions of cyber warfare. Many organizations and individuals has defined the concept of cyber warfare according to their identification methods, but there is no commonly accepted definition for the term (Ophardt, 2010) Lacking further clarification from these sources, a different approach to defining cyber warfare is possible by defining its subcomponents.

From the perspective of military operation, the term has been used to refer to violent conflict between adversaries to gain advantages on political and ideological issues. According to Junio (2013), cyber warfare can be described as an aggressive act that involves computer network attacks. In this context, a network attack refers to an act upon information for the purpose of destroying, degrading or disrupting.

A key component of cyber warfare is that it requires *physical impact*. Military experts call it a 'kinetic' effect (McGraw, 2013). For instance, attacking an enemy's command and control system by using software programs and taking control of the enemy's aerial vehicles such as unmanned aerial vehicles and drones and directing them to wrong targets can be considered as an example of cyber war. Within this framework, to be conceived as a cyber war practice, the tools can be virtual but the impacts must be physical.

The next section describes the terms war, cyber and cyber warfare in more detail.

## 2.2. War, Cyber, Cyberspace and Cyber Warfare

The definition of war goes back much early dates. Sun TZU described the war as: "The art of war is of vital importance to the State. It is a matter of life and death, a road either to safety or to ruin. Hence it is a subject of inquiry which can on no account be neglected". More recently, the description by Clausewitz (1832, On War) for war is as follows:

> *We shall not enter into any of the abstruse definitions of war used by publicists. We shall keep to the element of the thing itself, to a duel. War is nothing but a duel on an extensive scale. If we would conceive as a unit the countless number of duels which make up a war, we shall do so best by supposing to ourselves two wrestlers. Each strives by physical force to compel the other to submit to his will: his first object is to throw his adversary, and thus to render him incapable of further resistance. War*

> *therefore is an act of violence to compel our opponent to fulfil our will (p. 39).*

After the first use of the term cyber by Wiener (1948), in 1984, the term "cyberspace" was used in a science fiction novel by William Gibson (Whittekar, 2004). United Nations (UN) defines cyber as "the global system of systems of Internetted computers, communications infrastructures, online conferencing entities, databases and information utilities generally known as the Net." According to the report by Michael N. Schmitt, 2013, NATO defines cyber in Tallin Manual as; "…..connotes a relationship with information technology" (Tallin Manual on the International Law Applicable to Cyber Warfare, 2013). USA Department of Defense defines cyberspace as "… global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Department of Defense Dictionary of Military and Associated Terms, 2010). In summary, a broad analysis of the  definitions of cyber is related to technology, communication systems, internet and networks.

As mentioned in the previous section, there is no universally accepted definition of cyberwarfare. However, according to Andress and Winterfeld (2012), cyber attacks can be categorized in two main parts: Logical cyber attacks and Physical cyber attacks. Logical cyber attacks involve the attacks that employ recon tools, scan tools, access and escalation tools, exfiltration tools, assault tools, and obfuscation tools. Physical cyber attacks involve the ones that employ supply chain attack tools and SCADA (Infrastructure) attack tools.

Jeffrey Carr makes a description, inspired by Sun Tzu's writings, as "Cyber Warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood." (Carr and O'Reilly, 2012). The definition of cyberwar by the United Nations is as "a type of war in which computer systems are used to damage or destroy enemy systems."  Cyberwarfare involves actions directed at achieving informational superiority, may involve damaging a political, military or economic enemy's information and information systems or protecting one's own information and information systems. An example would be the destruction or corruption of a government or military organization. The Encyclopedia Britannica defines cyberwarfare (aka. cyber warfare) as "war conducted in and from computers and the networks connecting them, waged by states or their proxies against other states". Cyberwar is usually waged against government and military networks in order to disrupt, destroy or deny their use (McLaughlin, 2011).

Today, information technologies have been changing our way of communication, business mode, and also everyday life. Military conducts and affairs are affected by information technologies, as well. With the advent of cyber and cyber-related issues, military institutions have started to encounter cyber warfare and its inevitable implications on the war itself, since the information systems controlling our critical infrastructure may be vulnerable to cyber attack. A loss in a cyber war is therefore inevitable unless we improve our cyber defenses. The ideal way to do this is to build security into systems at the design stage (McGraw, 2013).

The next chapter introduces the development of the Lanchester Combat (Kinetic) Model, follow-up models, such as the Epidemic Model, and the Mixed Epidemic Models, that will provide the infrastructure for the proposed DDoS model in this thesis.

# CHAPTER 3

# MODEL GENERATION

## 3.1. Introduction

In this chapter, the two main elements of this study are defined: War and DDoS attacks. To model war, the Lanchester Combat (Kinetic) Model is introduced. To model DDoS attacks, the Epidemic Model differential equations are employed. Additionally, a Mixed Epidemic Model is proposed, which comprises both the Lanchester Combat (Kinetic) Model and the Epidemic Model, as a model that represents the interaction between war and DDoS attacks.

## 3.2. Differential Equations

Differential equations were applied firstly in battlefield modelling through the Lanchester models in the early 1900s. They were developed in order to better understand the air space that began to affect the ground battlefields (e.g.,Lanchester, 1916).

Lanchester (1916) formulated the original equations of combat between two opposing forces. After then, the formulations have been re-organized, extended and applied in other disciplines. The researchers used the formulas to develop research in specific disciplines (Bach, Dolansky & Stubbs, 1961). For instance, a combination of Lanchester models have been applied to investigayte the parameters that influence the force ratios in the guerrrila-countergerilla warfare (Deicthman, 1962).

Another area of the application of the Lanchester models is marketing. As an example, Kimball (1957) and Little (1979) emphasized the economic application of the equations. In their analysis, they proposed that competing firms always like to maximize their profits. A focus on the advertising competition between two rivals and advanced mathematical equations are needed to conclude specific results that give insights about how they would expect markets to develop in regards to advertising levels and market shares (Erickson, 1985).

The Lanchester models are ordinary differential equation (ODE) models that aims at explaining mutual attrition behavior in combat (Lanchester, 1916). The same methods have been used to understand the cyber space, which is conceived as a different dimension of war recently (Schramm & Gaver, 2013). In the present study, we model the effects of DDoS attacks on cyberwarfare scenarios by applying the Lanchester Model.

In DDoS attack modeling, an Epidemic Model, namely the S-I-R- model was employed in order to represent computers that will serve as means for spreading malware and launching DDoS attacks. The Epidemic Model is a configuration that was firstly developed in order to investigate the contagion of diseases (Kermack & McKendrick, 1927).

Cyber warfare does not have a single and commonly accepted mathematical model. In this thesis, our goal is to explore the effect of recovery by using closed form Lanchester models. We aim to capture the essence of exploiting vulnerabilities by spreading malicious code behavior of cyber operations by using ODE (ordinary differential equation) models of disease spread. The next section presents a mathematical description of the war and epidemic models, as well as the Mixed Epidemic Model that is used in the present thesis.

## 3.3. War and Epidemic Models

### 3.3.1. Lanchester Combat (Kinetic) Model

It is a traditional and fundamental issue in the military field to describe the warfare. In this study, we use the Lanchester Models as the core combat model. In a Lanchester model, two opposing sides attack each other and each side aims at reducing the opposing side's power. Despite its long history back to earlier times, the Lanchester Model has still been actively used as a mathematical model of warfare (e.g., Kim, Moon and Shin, 2017).

The Lanchester model has two subtypes: The Aimed-fire Model assumes that one element on one of the sides can only affect one element on the other side. In the other type, namely in the Area-fire Model, it is assumed that one element on one of the sides can influence more than one element on the other side. As a working assumption, we use only the Aimed-fire model of Lanchester Model. Figure 1 is a schematic representation of the Lanchester model.

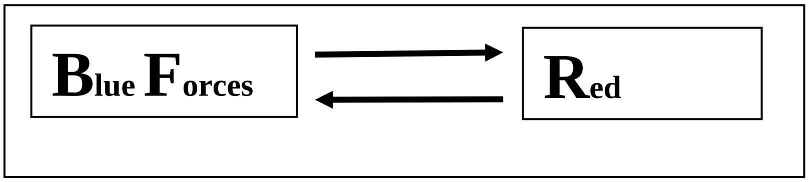


Figure 1. Lanchester Combat Model

Assuming that a blue force B (one of the sides) and a red force R (the other side) attack each other, the basic equation for the Aimed-fire Model is shown below;

$$\frac{dB(t)}{dt} = -\gamma R(t) \qquad (1)$$

where B(t) shows the force that Blue has at time t. $\frac{dB(t)}{dt}$ gives the ratio of change of the Blue force at a certain time. $\gamma$ (gamma) is the Red's kinetic attack rate, R(t) shows the force of Red has at time t. Similarly, we can formulate the change in the Red force as follows:

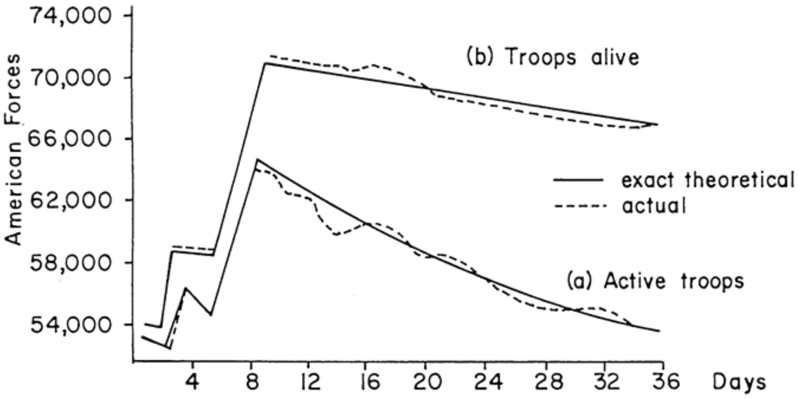
$$\frac{dR(t)}{dt} = -\delta B(t) \qquad (2)$$

where R(t) shows the force that Red has at time t. $\frac{dR(t)}{dt}$ gives the ratio of change of the Red force at a certain time. $\delta$(delta) is the Blue's kinetic attack rate. Finally, B(t) shows the force of Blue has at time t.

Since we use the Aimed-fire model, each and every attack that the Red launches means casualties in the Blue forces. The Red's effectiveness depends on the Red's kinetic rate and the number of Red's forces at time t. A similar case also applies to (2): Each and every attack the Blue force launches leads to casualties in the Red forces. The Blue's effectiveness depends on Blue's kinetic rate and the number of Blue's forces at time t. The exchange ratio of force at a certain time is a function of the attacker's amount of force and the attack rate.

The Aimed-fire model is one of the most applied subtypes of the Lanchester model. By applying this model, we can predict the results of conflicts, as well as making changes and adaptations.

The best example that this model was used was the prediction of the results of  the Battle of Iwo-Jima in 1945 (Engel, 1954).



Graphic 1. A Comparison of the Lanchester model outcome and real results for the 1945 Battle of Iwo-Jima (from Engel, 1954).

As Graphic 1 shows, Engel (1954) confirmed the Lanchester model in a specific battle. In the Iowa battle, there was a daily record of reinforcements and casualties of fighting sides. Based on these records, Americans got 54,000 reinforcements in the first day, 6000 troops in the third day and 13,000 troops in the sixth day. The attack rates of the sides were calculated and then formulated by (3) and (4).

$$\frac{dU(t)}{dt} = A(t) - XJ(t) \tag{3}$$

$$\frac{dJ(t)}{dt} = -YU(t) \tag{4}$$

In (3), U represents the American forces, J represents the Japanese forces, A represents the reinforcements and X stands for the attack rates of Japanese troops.  In this formula, $\frac{dU(t)}{dt}$ shows the abrupt change in the number of American troops. In (4), also, J represents the Japanese troops and U represents the American troops. Unlike the previous formula, Y stands for attack rates of the American troops. In this formula,$\frac{dJ(t)}{dt}$ shows the abrupt change in the number of Japanese troops.

Despite its strengths to predict the outcomes of the battles, as presented by historical evidence in the literature, the Lanchester model is not appropriate in its original form for modelling a DDoS attack. For this reason, the Mixed Epidemic Model is applied in this thesis. The Mixed Epidemic Model is a combination of the Lanchester Model and the Epidemic Model. In the next section, Kermack and McKendrick's (1927) Epidemic Model is introduced.

### 3.3.2. Kermack and McKendrick (1927) Epidemic Model

In Epidemiology, the most commonly used mathematical models are S-I and S-I-R. In these models, a population is divided into three categories.

- S stands for *Susceptible*
- I represents *Infected*
- R is *Removed* (see a Murray, 2002 for a sample implementation of the model in Epidemiology).

In the present study, we apply the S-I-R modeling since it is more compatible to cyberwarfare, by following Schramn and Gaver (2013), which applied the S-I-R model in cyber warfare studies (Figure 2).

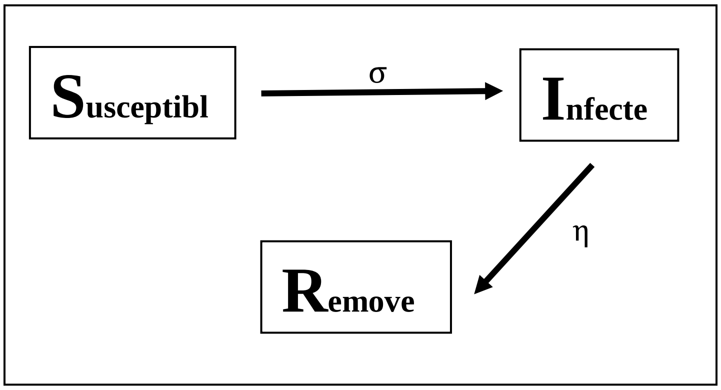


Figure 2: Schema of S-I-R Model

Computer malware are the similar to the viruses that infect human in certain aspects. In a human population, there are people who may be infected by viruses (cf. *Susceptible*), there are people who are infected by viruses (cf. *Infected*) and there are people who take precautions before getting infected or people who are treated after they are infected by viruses (cf. *Removed*). Similar conditions apply to computer terminology: Computers that may be infected by malware (cf. *Susceptible*), computers that are infected by malware (cf. *Infected*) and computers with anti-virus programs or computers that are cleaned up after being infected by malware (cf. *Removed*). In the present thesis we employ this similarity between human populations and computer populations by employing the S-I-R model.

Epidemiologic models are categorized according to the type of the spreading of the disease. In mathematical formulation, as stated in Kernack and McKerndrick's (1927), the model is:

$$\frac{\mathrm{dS(t)}}{\mathrm{dt}} = -\sigma\ \mathrm{S(t)}\ \mathrm{I(t)} \qquad (5)$$

where $\frac{\mathrm{dS(t)}}{\mathrm{dt}}$ gives the exchange ratio for the group that is vulnerable to the disease at time t. This exchange ratio depends on the relationship between the *Infected* group and the *Susceptible* group (i.e., the vulnerable group) and also the virus spreading speed σ (sigma). A similar formulation applies to the *Infected* group:

$$\frac{\mathrm{dI(t)}}{\mathrm{dt}} = \sigma\ \mathrm{S(t)}\ \mathrm{I(t)} - \eta\ \mathrm{I(t)} \qquad (6)$$

where the $\frac{\mathrm{dI(t)}}{\mathrm{dt}}$ represents the exchange ratio of the group that has been Infected by the disease at time t. This exchange ratio is found by extracting the total number of the two other groups from the whole population (i.e., the sum of S, I and R). The change in the Removed group is given below:

$$\frac{\mathrm{dR(t)}}{\mathrm{dt}} = \eta\ \mathrm{I(t)} \qquad (7)$$

The $\frac{\mathrm{dR(t)}}{\mathrm{dt}}$ is the exchange ratio of the group that has survived from the disease at t. This ratio is based on the Infection removed rate η (eta).

The Epidemic model has been further improved for its use in cyber warfare by Schramm and Gaver (2013). This model, namely the Mixed Epidemic Model is presented in the following section.

### 3.3.3. The Mixed Epidemic Model

The Mixed Epidemic Model, developed by Schramm and Gaver (2013) is a combination of the Lanchester combat model and the Epidemic model. The capital letters in the formulation stand for the exchange population through time, as described in the previous section. The original model has four formulas. The formula below describes the change in the ratio of the whole population:

There two forces; Red and Blue. Blue Forces is subdivided three groups; Susceptible (S), Infected (I) and Removed (R). The Susceptible group have not been affected by malware. The Infected group have been affected by the malware and the Removed group is the one that the malware has been removed. All the groups attack to Red Forces with β Attack Rate. However, the Infected group's Attack Rate ($\beta_d$) is smaller than the Susceptible group and the Removed group's Attack Rate ($\beta_u$). The malware influences the Blue Force's attack effectiveness. The Red Forces attack to the Blue Forces with an Attack Rate (γ).

Where $\frac{dZ(t)}{dt}$ is the number of the whole Red Forces, $\frac{dS(t)}{dt}$ stands for the number of Susceptible units in the whole population at time t, $\frac{dI(t)}{dt}$ stands for the number of the Infected units in the whole population at time t and $\frac{dR(t)}{dt}$ stands for the number of Recovered "(patched) in the whole population at time t. We use the following formulae for the model.

$$\frac{dZ(t)}{dt} = -\beta_u\big(S(t) + R(t)\big) - \beta_d I(t) \qquad (8)$$

$$\frac{dS(t)}{dt} = -\varepsilon\, S(t)I(t) - \eta\, S\,(t)R(t) - \gamma\, Z(t)\frac{S(t)}{S(t) + I(t) + R(t)} \qquad (9)$$

$$\frac{dI(t)}{dt} = \varepsilon\, S(t)I(t) - \eta\, I(t)R(t) - \gamma\, Z(t)\frac{I(t)}{S(t) + I(t) + R(t)} \qquad (10)$$

$$\frac{dR(t)}{dt} = \eta\, S(t)R(t) + \eta\, I(t)R(t) - \gamma\, Z(t)\frac{R(t)}{S(t) + I(t) + R(t)} \qquad (11)$$

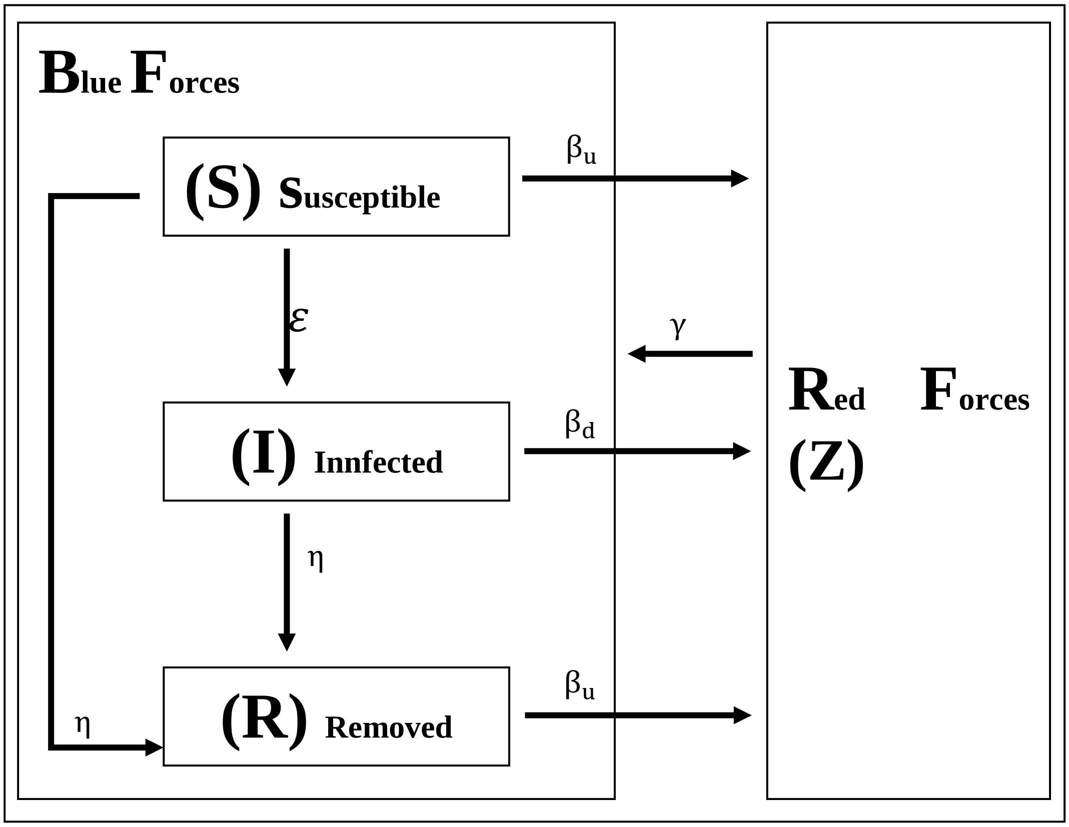


Figure 3: Mixed Epidemic Model

In Section 3.3, the Lanchester Combat (Kinetic) Model that is used in modeling wars and conflicts, the Epidemic Model that is used in modeling epidemics, and the Mixed Epidemic Model that is a combination of both previous models, are explained. The purpose of the present study is to model the DDoS attacks by applying the Mixed Epidemic Model.

The present study investigates how cyber war capability, as modelled by the Mixed Epidemic Model, can be influenced by the physical war. An influence is already expected when the computers that carry out the cyber war are also actively involved in the war. On the other hand, in our model, the cyber war is unaffected since it is initiated by a neutral, White Country.

Moreover, DDoS attack rates can be independently updated regardless of the effects of war. In its original form, the Mixed Epidemic Model has no such a capability. In the present study, we improve the Mixed Epidemic Model for this capability. Before presenting the model itself, the next section presents the DDoS concept as a background for the proposed model.

### 3.4.Distributed Denial Of Service (DDoS) Attacks

Cyber attacks may aim at deteriorating an organization’s network services with denial of service (DoS) attacks and damaging an organization’s reputation in the market. Since there are such hazardous malware attacks, organizations have to decide whether they should have a passive defense stance or act more aggressively such as starting a counter attack against their attackers (McLaughlin, 2011). Based on the definition from the study of Singleton (2006), Distributed Denial of Service (DDoS) is defined as a malicious software attack tactic that aims to destroy the capabilities of a network-bases service, such as a website, by accessing a vulnerable computer and through that opening sending an excessive number of packets of information to target networks over the network.

In 1999, the University of Minnesota declared that they faced a DDoS attack and this incident has been recorded as the first publicly reported appearance of DDoS attack (Garber, 2000). Since then, DDoS attacks have become popular. Recently, DDoS attacks can be organized by relatively easily accessible tool sets for inexperienced attackers, thus leading to higher costs for business environments (Molsa, 2005). Another remarkable incident that captured the press attention took place in Estonia. Starting on April 27, 2007 many Estonian websites were under constant DDoS attacks and they lasted for three weeks. Meanwhile, Estonia and Russia were engaged in a crisis over the removal of a Soviet war memorial, known as the Bronze Soldier of Tallinn, in Estonia. Estonia changed the location of the war memorial on April 27 and it sparked vigorous protests among ethnic Russians. Estonian law enforcement arrested 1300 ethnic Russians. Since DDoS attacks came to surface just after the relocation of war memorial, the crisis was thought to be rationale for the attacks (Chen, 2010).

In 2012, distributed denial of service (DDoS) attacks were carried out against the New York Stock Exchange and a number of banks, including J.P. Morgan Chase. Credit for these attacks was claimed by a hacktivist group called the Qassam Cyber Fighters, which have labeled the attacks “Operation Ababil.” The attacks had been executed in several phases and were restarted in March 2013. The size of the attacks (65 gigabits/second) is more consistent with a state actor than with a typical hactivist DoS attack (~2 gigabits/ second) (Gonsalves, 2012).

On December 14, 2015, the servers in the Middle East Technical University, Turkey, were attacked by DDoS that lasted almost two weeks. During the attacks, several financial establishments, government institutions and civil sector companies suffered blockage and issues to connect to world wide web and other internet applications. To sum up, DDoS attacks comprise an active domain of cyber warfare both at national and international level.

There are multiple ways of designing a DDoS attack: to nullify the target servers with packets in order to keep the servers unresponsive to legitimate packets. A typical way of doing this is to send the servers much more request for information than they can handle. This situation will overburden the computers, thus system admins might have to take them offline to counter the attacks. Unfortunately, most of the systems connected to the Internet are vulnerable to DDoS attacks and they are typical open targets for malicious software (Leiner, 2003).

According to Thiruvaazhi and Alex (2012), Distributed Denial of Service (DDoS) is the number one security issue that consumes time and financial resources of organizations. Since the Internet is a public resource that is available to anyone, and vulnerabilities are indispensable, finding effective solutions to DDoS attacks remain an open and continuous problem. The market research company Forrester conducted a study in 2009 and reported that 74% of information technology companies counter DDoS attacks in a one-year period, despite their security controls (cited in Schramm and Gaver, 2013). The company also reported that DDoS attacks are at top of the list of security issues wasting valuable time and resources of the organizations. 31% of these attacks resulted in unavailable service and many organizations suffered significantly high revenue during that process until restoration.

The main purpose of a DDoS attack is straightforward, namely to make a service unavailable to authorized users. What makes a DDoS attack complex is related to identification of the original source (Thiruvaazhi and Alex, 2012). DDoS attacks are generally conducted by attackers who aim at accessing main servers and attackers scan the Internet and identify vulnerable computers. These vulnerable machines are called by several names, such as agents, slaves, zombies or botnets. Then, by exploiting these agents, attackers establish channels for communication and send the attacking codes to their target computers (Zaroo, 2002).

Considering complex features of a DDoS attack, defense applications against DDoS must include "defense-in-depth" principles (Mirkovic and Reiher, 2004). In order to deter malicious software programs and other worms and alleviate their reverse impacts, organizations should implement a defense strategy that consists of echeloned mechanism that will make it difficult for attackers to infiltrate. In terms of a private organization, this infrastructural cyber defense mechanism can include passive tools such as antivirus software programs, access controls, firewalls and identity management applications (McLaughlin, 2011).

Leiner (2003) states that DDoS attacks are inevitable and the security problems constitute major obstacles to the development of network systems. DDoS attacks are recently among most problematic issues in network security threats. DDoS attack is an offensive action on survivability and availability in the Internet, other infrastructures and wireless networks as well (Gupta, Joshi & Misra, 2009).

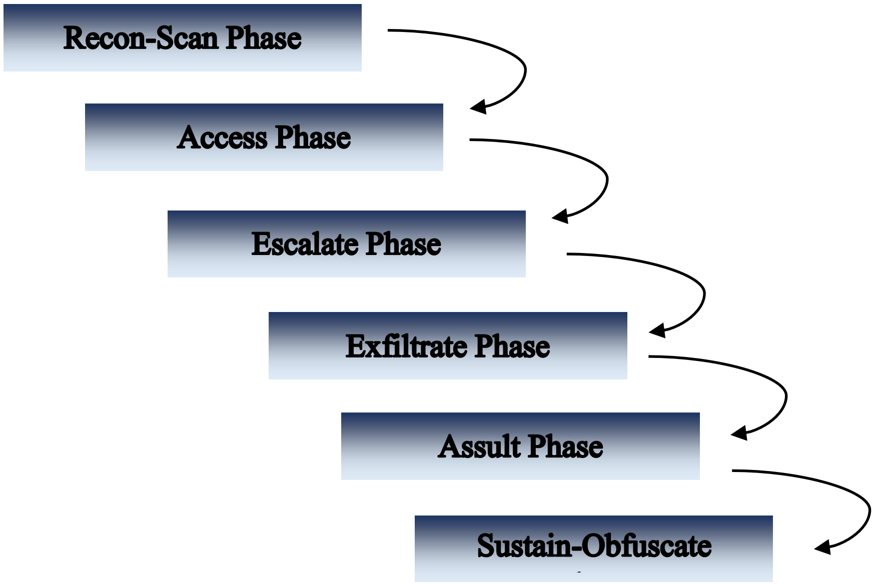


Figure 4. DDoS Attack Phases

This thesis focuses on the relationship between DDoS attacks and physical attacks. A typical pattern in a DDoS attack starts with "Reconnaissince and Scan phases". These are essential to collect information and intelligence for further phases. Next part is the "Access phase", which is the intrusion to the target network. Then comes the "Escalation phase", to gain the authority in the network for further actions. Even after gaining the administrator level authority, the DDoS attack is not ready to start yet, because defensive mechanisms in networks filter some actions. Here the intruder takes "Infiltration" actions to clear the path for further actions and to detach the target data. Now the DDoS attack can be ignited in the "Assault phase". After the attack starts, sustainment actions are required. Finally, before finishing the attack, the intruder clears all the information and traces that was left since the scan phase in order to hide the source. (Andress and Winterfeld, 2012)

In the proposed model, we simplify these processes to access, infiltration and assault with related parameters. In particular, we simplify the model to narrow down the scope of the study, by leaving the expansion to further research. In this context, for any type of cyber attack (including web defacement attacks, DOS attacks, zero-day attacks, malicious code attacks etc.) for a closed network as a military network, malicious code needs to be used for access, escalate or assault phases. Accordingly, we use epidemiology to model cyber infection for these three phases, and the model involves three phases: Access, Escalate and Assault. In this case, we assume that Recon and Scan phases were already completed, and we assume no evidence of the existence of the other phases.

The proposed model is a model for a Distributed Denial of Service (DDoS) attack, which uses infection spread in an external network. A DDoS attack is an indirect attack type, which intends to decrease the usable capacity of communication networks by sending constant messages and by generating a heavy burden of unnecessary message traffic. So, DDoS networks (or botnets) attack a given target with brutal cyber force as a physical attack and reduce the capacity to communicate.

In the present study, the DDoS attack is conducted by neutral White population by applying malware programs prepared by Blue Forces. The reason behind the use of a neutral White population force is that it is the cheapest Use of white population is the cheapest and the most common way conduct a cyber attack. Also, there are a few recent incidents in real world that shows these types of attacks can be used with a kinetic attack (before or after a kinetic battle starts).

In Chapter 4, our model is reported. The formulas and the results are analysed.

# CHAPTER 4

# THE MODEL

## 4.1. A Description of the DDoS Attack on Kinetic Battle Model

In this model, we study the effects of a DDoS attack on a kinetic battle. Based on our model design, we assume that only one of the sides can organize and run DDoS attacks.

There are three forces in the model. The model assumes that a malicious code, which is known as malware, is introduced by the Blue force and it is spread between the computer systems of a neutral country, in this case the White force. The White force includes three separate groups of population, namely the *Susceptable* group, the *Infected* group, and the *Removed* group. More details about those groups will be presented below.

The method of malware spreading was simulated by the Epidemic model, which was introduced in the previous sections. On the other hand, the cyber attacks between the Blue side and the Red side were simulated by the Lanchester model (Lanchester, 1916).

The parameters of the model, by definition, are the attack rate and the number of initial forces. We made the following initial assumptions for the parameter setting of the model.

- The two forces (Blue, Red) start to attack each other by time 0 (t=0)
- The number of the Blue forces (B) decreases due to the kinetic attack rate of the Red forces (γ / gamma)
- The number of the Red forces (R) decreases due to the kinetic attack rate of the Blue forces (δ / delta)

- The Infected group in the White forces (i.e., botnets)[2] initiate the DDoS attacks, thus attacking the Red forces.

- The malware (i.e., the malicious code) spreads with the rate (σ / sigma) and the infection is removed by the rate (η / eta) in the White forces.

- The efficiency rate (λ / lambda) of the DDoS attack is scaled between 0-1.

Table 1 shows the components used in the model.

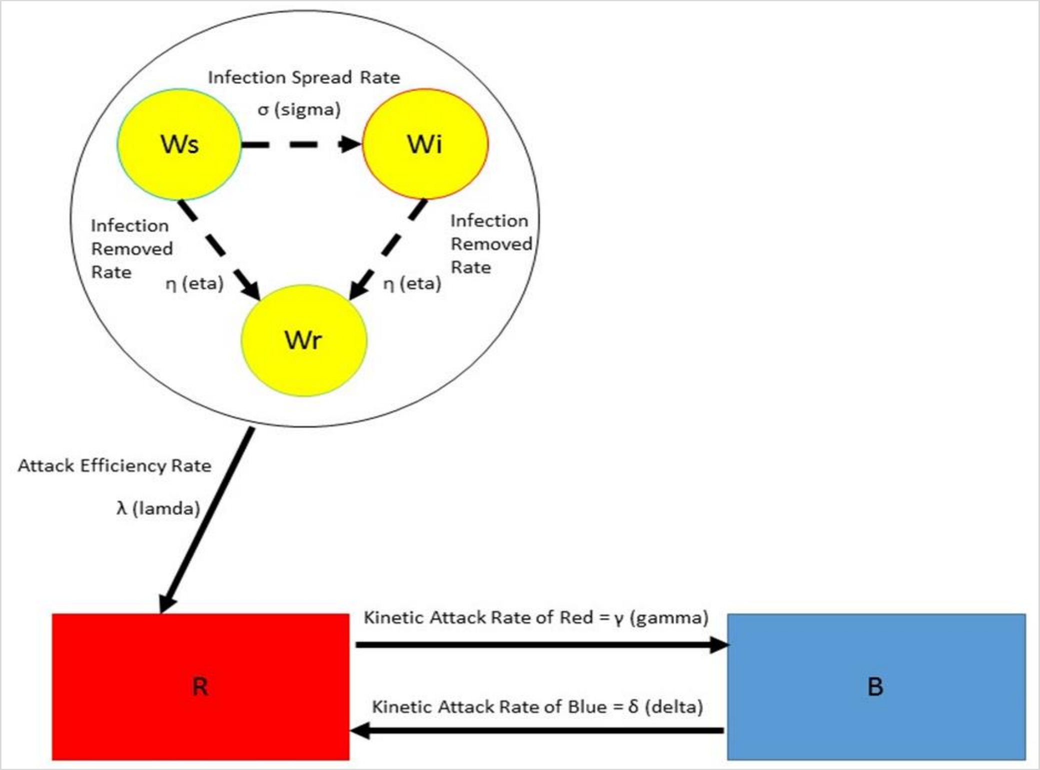
| **Component** | **Symbol** |
|---|---|
| Blue Forces | B |
| Red Forces | R |
| White Population | W |
| White Susceptible | Ws |
| White Infected | Wi |
| White Removed | Wr |
| Kinetic Attack Rate of Red | γ (gamma) |
| Kinetic Attack Rate of Blue | δ (delta) |
| Infection Spread Rate | σ (sigma) |
| Infection Removed Rate | η (eta) |
| Attack Efficiency Rate | λ (lambda) |

Table 1: The components the model.

The model is depicted in Figure 5.

[2] Botnet: A collection of devices which are internet connected. PCs, servers, mobile devices etc. that are infected and controlled by a malware.

Figure 5: A simplified representation of DDoS Attack on Kinetic Battle Model



In Figure 5, the Red forces are represented by the red box (R) and the Blue forces are represented by the blue box (B), and the three groups in the White forces (Ws, Wi, Wr) are represented within the circle. The subpopulations under the White forces (i.e., the Susceptible group Ws, the Infected group Wi, and the Recovered group Wr) are represented by smaller circles. The solid lines show the effects from a force to another force (W, B, R). The dotted lines show the flow of the group population from one state to another state (Ws, Wi, Wr). Table 2 shows the population flow rates from a state to another state.

Table 2 shows the population flow rates (Within groups among white population )

| | **Ws** | **Wi** | **Wr** |
|---|---|---|---|
| **Ws** | - | σ (sigma) | η (eta) |
| **Wi** | - | - | η (eta) |
| **Wr** | - | - | - |

Table 2: Flow Rates

Table 3 shows the population flow rates from a force to another force.

| | **W** | **B** | **R** |
|---|---|---|---|
| **W** | - | - | λ (lambda) |
| **B** | - | - | δ (delta) |
| **R** | - | γ (gamma) | - |

Table 3: Effect Rates

## 4.2. Assumptions

The design of the model requires the use of a set of assumptions, as presented below.

The model involves three different forces (Red, Blue, White). The population of the three forces is equal at the beginning. More specifically, we assume that each force is composed of 1000 units. Within the context of cyberwar, our units correspond to computers. During the course of the cyberwar, we assume that the numbers in the Red forces and the numbers in the Blue forces decrease, whereas the number of units in the White forces remain the same. In other words, we have simplified the original S-I-R model (see Chapter 3) by assuming that the white population, namely W= Ws(t) + Wi(t) + Wr(t) stays constant in time, where

- Ws(t) stands for the number of unit (i.e., the population) that has not been Infected yet or that has not been Removed at time t.

- Wi(t) is the population that has been Infected by the virus at time t.

- Wr(t) stands for the number of groups that has been Infected by the virus and then Removed or the group that has been Removed although it has never been Infected.

The sum of those three groups above represents the whole population of the White forces.

We assume that the virus was injected to the White forces by the Blue forces, thus resulting in the Wi group within white forces. So, the Blue forces are able to install malware in White forces' computers. We also assume that the DDoS attack is performed only against the Red forces by the White forces. We further assume that the injected virus starts spreading when the attack starts, and the virus does not spread before the attack. Moreover, there are no countermeasures to prevent virus spread before it is activated.

Among 1000 units per forces, we assume that the 1000 units in the White forces are all active at all the time. When the cyberwar start, the Infected group Wi affects the Susceptible group Ws by the spread rate σ (sigma), and the Removed group Wr units clean (and immunize) other infected or susceptible units (Wi, Ws). In other words, the new units in the Removed group come from either the Susceptible group Ws or by the Infected group Wi.

As presented in Chapter 3, the Lanchester model involves two sub-types, namely the Area-Fire Model and the Aimed-Fire model.  In the present study, we assume the Aimed-Fire model, in which each fire is directed to live targets (in this case, active units). We assume that each force whether it is Red, Blue or White, fight under homogeneous conditions. For each force, we can assign a kill rate per instant of time (dt), Kinetic Attack Rate of Blue δ (delta) ve Kinetic Attack Rate of Red γ (gamma) attack rates. We do not assume any defense rate. The attack rate stays constant during the cyberwar. There are no independent rates for kinetic defense, environmental effects, tactics, moral effects etc., so we use an average attack rate with all these considerations. Also, there are no independent rates for cyber defense, communication infrastructure resiliency, Anomaly Detection System (ADS) effect etc., so we use an average efficiency rate with all these considerations.

In the model, the Red Forces and the Blue Forces are fighting and the White Forces only initiate the DDoS attacks. That is, the White Forces' DDoS Attack Efficiency Rate is different than the Red Forces' Kinetic Attack Rate and the Blue Forces' Kinetic Attack Rate.

We run the model in R programming environment and investigated the changes in the Blue forces and the Red forces in order to understand how a DDoS attack influences the results of a kinetic battle under certain assumptions. For this, we have generated a mathematical model that consisted of six differential equations, as presented below.

Three differential equations set the model for a military operation and the attrition behavior (cf. the Lanchester model). The remaining three equations comprise a model for a DDoS attack. The two groups of models are related by Infected group (Wi) in the White forces. The first differential equation, as shown by the formula below, represents the population (i.e., the number of units) change in the Blue forces.

$$\frac{\mathrm{dB(t)}}{\mathrm{dt}} = -\gamma\left(1 - \lambda\,\frac{Wi(t)}{\mathrm{W}(t)}\right).\mathrm{R(t)} \qquad (1)$$

So, the first equation means that the multiplication of three factors give us the change in the number of Blue force units per timeframe. The components of the multiplication involve a fixed coefficient, a variable coefficient and the number of Red force units per timeframe. The fixed coefficient represents the attack rate (kill probability) of each Red unit (γ gamma). The variable coefficient represents the attack efficiency rate of Red forces because they are affected by a DDoS attack with a different scale per timeframe. These coefficients are unitless and when multiplied by the number of Red, it gives the number of Blue attrition in that specific timeframe. λ (lambda) is the Attack Efficieny Rate of the DDoS attack and it is stable duruing the battle.

The second differential equation below shows the rate of change in Red forces.

$$\frac{\mathrm{dR(t)}}{\mathrm{dt}} = -\delta \,.\, \mathrm{B(t)} \qquad (2)$$

The components of the equation involve a fixed coefficient (attack rate of Blue δ (delta)) and the number of Blue force units per timeframe. Since the Blue forces are not affected by the DDoS attack, the variable coefficient is not necessary in this formulation.

The third equation means that the change in the number of White forces per timeframe, which is set to zero, as an assumption that was presented above. This is an assumption that no DDoS population changes from the beginning to the end of the conflict.

$$\frac{\mathrm{dW(t)}}{\mathrm{dt}} = 0 \qquad (3)$$

The following set of formulae shows the three differential equations together to represent the kinetic effects of the war model:

$$\frac{\mathrm{dB(t)}}{\mathrm{dt}} = -\gamma\left(1 - \lambda\, \frac{\mathrm{W_I}(t)}{\mathrm{W}(t)}\right).\,\mathrm{R(t)} \qquad (1)$$

$$\frac{\mathrm{dR(t)}}{\mathrm{dt}} = -\delta \,.\, \mathrm{B(t)} \qquad (2)$$

$$\frac{\mathrm{dW(t)}}{\mathrm{dt}} = 0 \qquad (3)$$

The second part of the model involves three differential equations that represent the DDoS attack by employing the Kermack-McKendrick disease spread model, which is used to define the virus spread and the cleaning process in a network. In this model, the white population does not have any kinetic relation with the others since there is no attack against the White forces. Therefore, the total population change will be 0. However, the Blue forces and the Red forces affect (kill) each other. The effect of the White forces is the reduction in the attack capability of Red.

The two important components in this formulation are Wi, which represents the Infected group in the White forces (i.e., the attacker bots in a DDoS attack) and the lambda which represents the effectiveness of each attacker unit in Wi. Observing the results of this type of effectiveness is important because as the effectiveness increase, the probability to hide the botnet goes down and results in a decrease in the DDoS attack impact. Also, setting a lower value for lambda results in a decrease in the DDoS attack impact.

However, an optimal value can be calculated for each variable. For the lambda parameter, we assumed 0.25 for the base case. The base is the situation in which none of the two forces (Red or Blue) are able to beat each other. The three differential equations in the second set show the rate of change of each sub-group (Ws, Wi, Wr) in the White forces, where the total population of the White forces is represented by a closed state $\mathrm{W} = \mathrm{W_S} + \mathrm{W_i} + \mathrm{W_R}$.

$$\frac{\mathrm{dW_S}}{\mathrm{dt}} = -\sigma \mathrm{W_S W_i} - \eta \mathrm{W_S W_R} \qquad (4)$$

$$\frac{\mathrm{dW_I}}{\mathrm{dt}} = +\sigma \mathrm{W_S W_i} - \eta \mathrm{W_i W_R} \qquad (5)$$

$$\frac{\mathrm{dW_R}}{\mathrm{dt}} = +\eta \mathrm{W_S W_R} + \eta \mathrm{W_i W_R} \qquad (6)$$

Also, these equation sets sum up to 0, since there is no change in total number of the units in the White forces.

The next step in our analysis is to examine our model in a simulated situation. For this, we generated simulation data, since the analysis of real-world data is beyond the scope of the present study due to practical difficulties in data availability in the domain of military applications and systems. We present our simulation in the following section.

### 4.3. Running the Model

For the analysis of the model, we designed test cases, in which we update the value of the model parameters. Information about the graphs has been presented on the same pages with the graphs.

Firstly, the variables have been presented at a table. Final graphs which were obtained by applying the variables were also presented under the table. The first five graphs were made in order to show how a variable affects the results. The variables were taken as base cases in the fifth graph where both sides didn't have superiority on the other. In the following graphs, each variable was presented compared to the base cases to understand the impacts on the results. While creating the graphs, first of all, Infection Spread Rate σ (sigma) was increased by 25% and its impacts on the results were recorded. Then, in order to have the same impact, there was a search to understand how much Kinetic Attack Rate of Blue δ (delta) should be increased. The same comparisons were also made between the Infection Removed Rate η (eta) and Kinetic Attack Rate of Red γ (gamma). Infection Spread Rate σ (sigma) and Infection Removed Rate η (eta) variables were increased 25%, 50%, 75% and 100% respectively and the results were then analyzed.

Two graphs were generated in order to enter data for running simulations. The first graph shows the population change of Red and Blue at a unit time. The second graph illustrates the change of Susceptible (Ws), Infected (Wi) and Removed (Wr) in White population throughout time.

Overall, there are 21 cases. The cases 1,2 and 3 indicate the results when there was no DDoS attack. The Case 4 stands for the results of the war when there was a conflict. The Case 5 was created as a base case. The other cases are created for investigating the effects on the results when each variable is updated at different rates.

After generating the 21 cases, the Attack Efficiency Rate λ (lambda) was calculated by assigning 10% to 100% (at 10% intervals). The results were then placed into one graph. In the Base case, this ratio was assumed to be as 0.25. Finally, all the changes and effects on the results were combined and presented on a table all together. To sum up, the variables are presented in the tables and graphs are generated as well as descriptions beneath them.

Before proceeding with the graphs, we present the within a story context, in order to improve its understandability: Red and Blue Forces are at war. White Forces are neutral. The Blue Forces install malware into White Forces' computers before the war so that malware initiates DDoS attacks against Red Forces when the war starts.

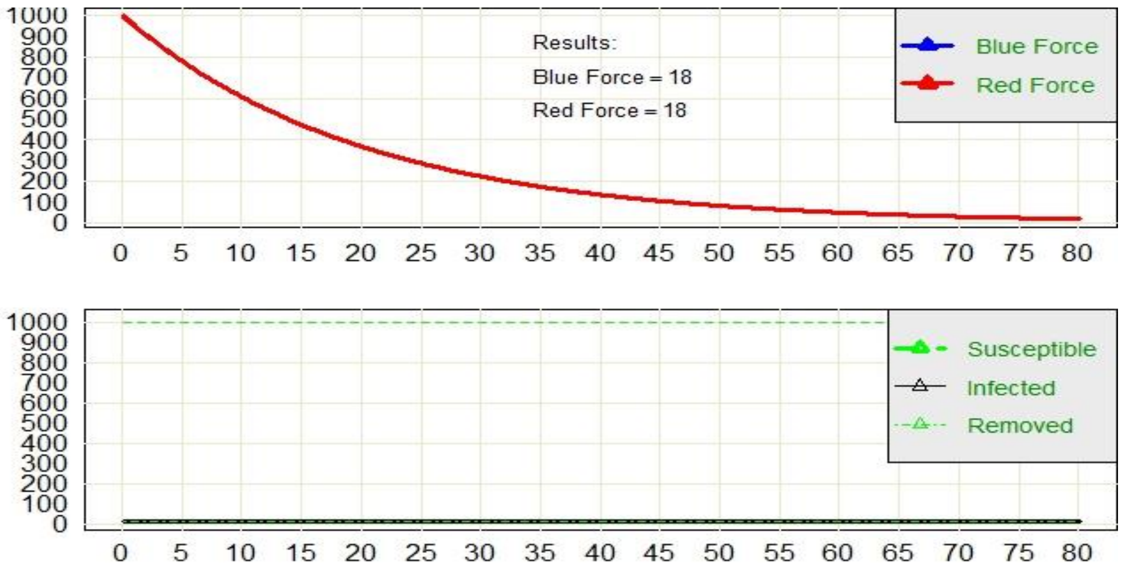
When Red and Blue forces wage war against each other, malware installed at White Force computers initiate the DDoS attacks against the Red Forces. For instance, during the Red-Blue fight, the DDoS attacks against Red Information Systems Infrastructure that enables Red forces communications, prevent Red troops communication abilities.

Although Red Intelligence units locate the Blue Forces frontier units, they cannot provide info to the units due to the slowdown in communication systems. Therefore, Red's Kinetic Attack Rate decreases and reduces damage to the Blue Forces. A similar example may also be given for air defense systems. For instance, the Blue Air Forces attack the Red Forces' Air Defense Systems and in the meanwhile botnets in the White Forces initiate DDoS attacks against the Red Forces in order to eliminate their air defense systems. Due to the slowdown in the Red network systems, they cannot detect air attacks or take necessary precautions even if they detect the attacks. And this situation prompts vulnerability in the Red's air defense systems and decreases the kinetic attack rate of the Red Forces.

**Case 1;** The variables are presented below. Because we have assigned the same variables to both forces, we are not anticipating any superiority of one on the other. Since Infection Spread Rate σ (sigma) and Infection Removed Rate η (eta) variables are taken 0.00, no changes are predicted in the second graph that illustrates the spread of the virus.

| **Kinetic Attack Rate of Blue δ (delta)** | **Kinetic Attack Rate of Red γ (gamma)** | **Infection Spread Rate σ (sigma)** | **Infection Removed Rate η (eta)** | **Attack Efficiency Rate λ (lambda)** |
|---|---|---|---|---|
| 0.050 | 0.050 | 0.00 | 0.00 | 0.00 |

Table 4: Table of Rates



Graphic 2: Graph of Results and Malware Spread

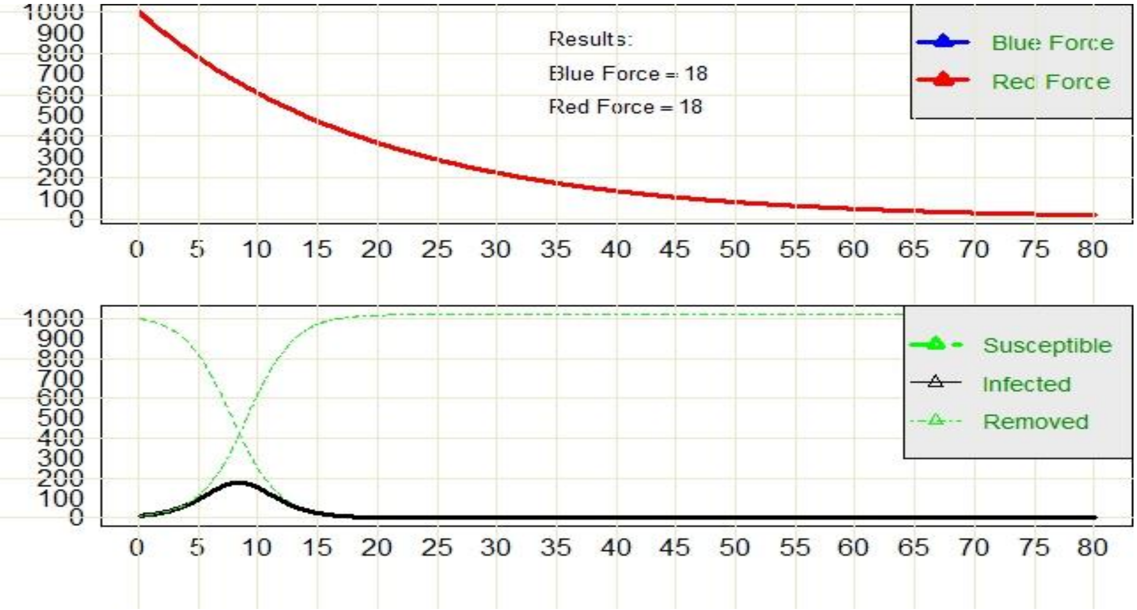
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are taken as 0.050. Since the populations and attack rates of the both sides are the same, no superiority on both each other took place. The graph was terminated at a certain point since it continues forever.

In the second graph, since the Infection Spread Rate σ (sigma) and the Infection Removed Rate η (eta) variables are 0.00, there is no change in the graph. The Ws is still 1000. Wi and Wr variables are 0.00 since there is no malware spread.

**Case 2;** The variables are presented below. Since we have assigned the same variables to both forces, we are not anticipating any superiority on each other. Also Infection Spread Rate σ (sigma) and Infection Removed Rate η (eta) variables are the same, malware might spread however, since Attack Efficiency Rate λ (lambda) is 0.00, it may not have affect the results.

| **Kinetic Attack Rate of Blue δ (delta)** | **Kinetic Attack Rate of Red γ (gamma)** | **Infection Spread Rate σ (sigma)** | **Infection Removed Rate η (eta)** | **Attack Efficiency Rate λ (lambda)** |
|---|---|---|---|---|
| 0.050 | 0.050 | 0.0005 | 0.0005 | 0.00 |

Table 5: Table of Rates



Graphic 3: Graph of Results and Malware Spread

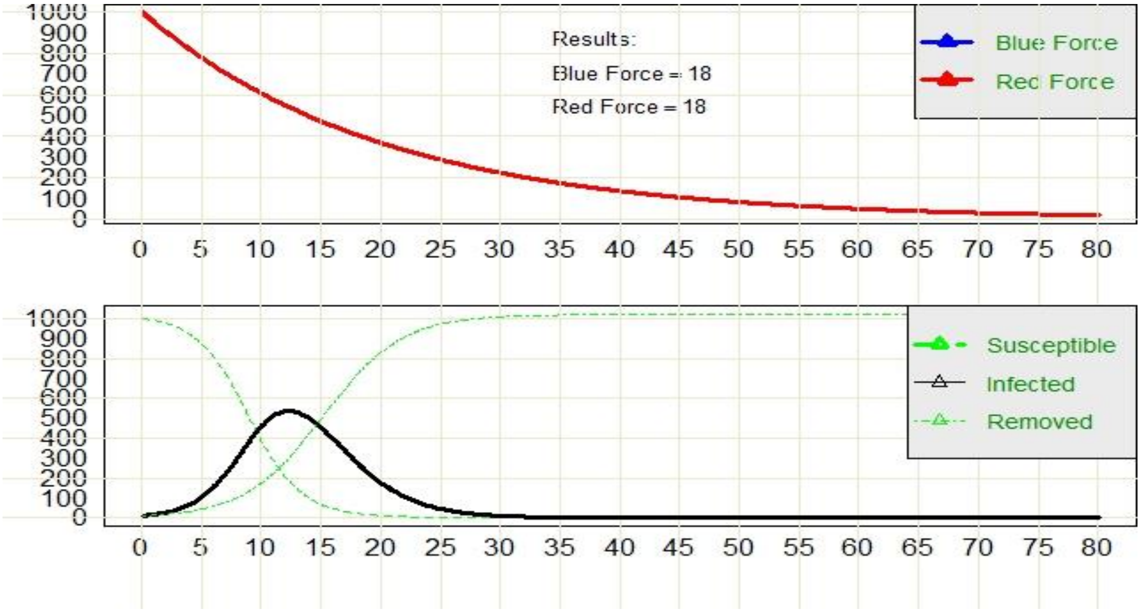
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are taken as 0.050. Since the populations and attack rates of the both sides are the same, no superiority on both each other took place. The graph was terminated at a certain point since it continues forever.

In the second graph, because the Infection Spread Rate σ (sigma) and the Infection Removed Rate η (eta) variables are the same, the system was affected by the malware (roughly 200), but later on malware was eradicated.

**Case 3;** The variables are presented below. Because we have assigned the same variables to both forces, we are not anticipating any superiority on each other. The Infection Spread Rate σ (sigma) and the Infection Removed Rate η (eta) variables are different. Because the Spread Rate is higher than Removed Rate, malware can spread more than previous conditions and it is predicted that it will not affect the results because the Attack Efficiency Rate λ (lambda) is 0.00.

| **Kinetic Attack Rate of Blue δ (delta)** | **Kinetic Attack Rate of Red γ (gamma)** | **Infection Spread Rate σ (sigma)** | **Infection Removed Rate η (eta)** | **Attack Efficiency Rate λ (lambda)** |
|---|---|---|---|---|
| 0.050 | 0.050 | 0.0005 | 0.0003 | 0.00 |

Table 6: Table of Rates



Graphic 4: Graph of Results and Malware Spread

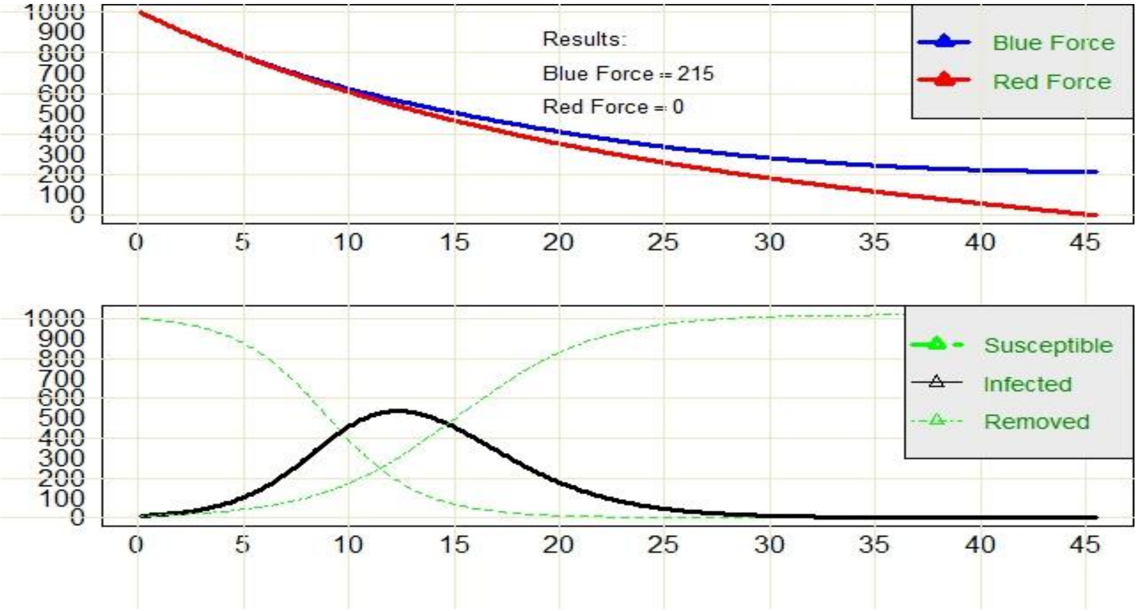
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are taken as 0.050. Since the populations and attack rates of the both sides are the same, no superiority on both each other took place. The graph was terminated at a certain point since it continues forever.

In the second graph, the Infection Spread Rate σ (sigma) is higher than the Infection Removed Rate η (eta). Malware inflected the system more compared to the previous conditions (roughly 570), but later on malware was eradicated.

**Case 4;** The variables are presented below. Both variables for two forces are the same however the Attack Efficiency Rate λ (lambda) is in favor of Blue, therefore Blue is expected to win. The Infection Spread Rate σ (sigma) and the Infection Removed Rate η (eta) variables are different. Because the Spread Rate is higher than the Removed Rate, malware is expected to be the same with the previous conditions.

| Kinetic Attack Rate of Blue δ (delta) | Kinetic Attack Rate of Red γ (gamma) | Infection Spread Rate σ (sigma) | Infection Removed Rate η (eta) | Attack Efficiency Rate λ (lambda) |
|---|---|---|---|---|
| 0.050 | 0.050 | 0.0005 | 0.0003 | 0.25 |

Table 7: Table of Rates



Graphic 5: Graph of Results and Malware Spread

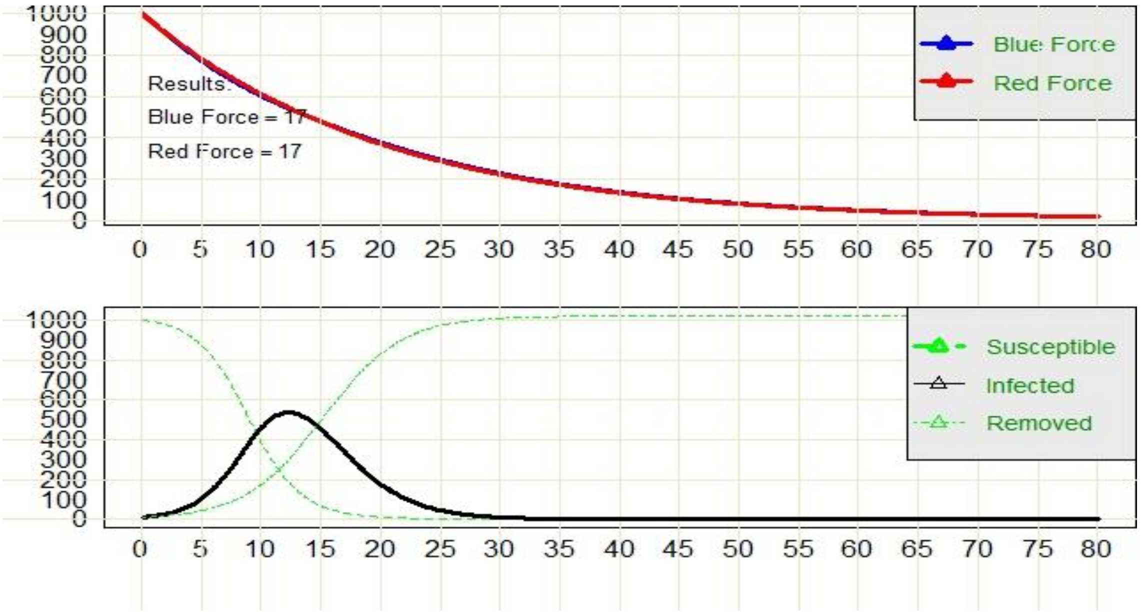
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are taken as 0.050. The populations and attack rates of the both sides are the same, but the Attack Efficiency Rate λ (lambda) is in favor of the Blue, that's why, the Blue has won.

In the second graph, the Infection Spread Rate σ (sigma) is higher than the Infection Removed Rate η (eta). Malware remains the same compared to the previous conditions and spreads equally to the system (roughly 570), but later on malware was eradicated.

**Case 5;** The variables are presented below. Both forces are assigned different variables. The Attack Efficiency Rate λ (lambda) is activated. The Infection Spread Reta σ (sigma) and the Infection Removed Rate η (eta) variables are different.

| Kinetic Attack Rate of Blue δ (delta) | Kinetic Attack Rate of Red γ (gamma) | Infection Spread Rate σ (sigma) | Infection Removed Rate η (eta) | Attack Efficiency Rate λ (lambda) |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |

Table 8: Table of Rates



Graphic 6: Graph of Results and Malware Spread

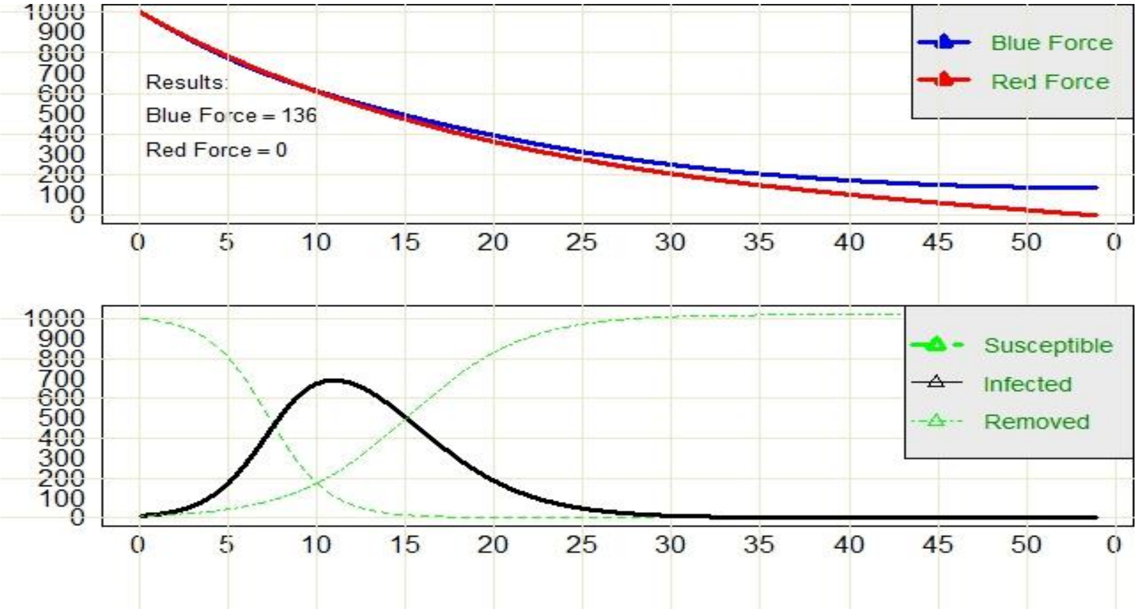
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are assigned differently. In the second graph, the Infection Spread Rate σ (sigma) is higher than the Infection Removed Rate η (eta). Malware remains the same compared to the previous conditions and spreads equally to the system (roughly 570), but later on malware was eradicated.

The Kinetic Attack Rate of Red γ (gamma) is higher than the Kinetic Attack Rate of Blue δ (delta), but, because the Attack Efficiency Rate λ (lambda) is active, both sides could not have superiority on each other. These conditions are taken as "Base Case". In the following analyses, variable comparisons are made based on the base cases.

**Case 6;** The variables are presented below. The Infection Spread Reta σ (sigma) is increased by 25%. Other variables are the same with base case.

| Kinetic Attack Rate of Blue δ (delta) | Kinetic Attack Rate of Red γ (gamma) | Infection Spread Rate σ (sigma) | Infection Removed Rate η (eta) | Attack Efficiency Rate λ (lambda) |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.052371 | 0.000625 | 0.0003 | 0.25 |

Table 9: Table of Rates



Graphic 7: Graph of Results and Malware Spread

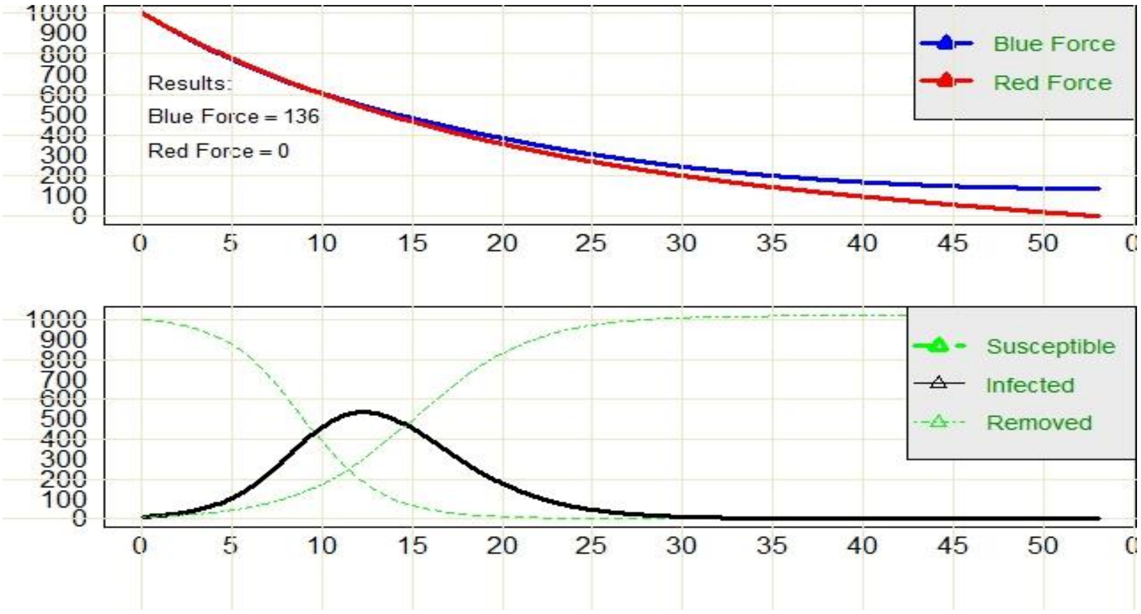
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are the same with the base case. The Infection Spread Rate σ (sigma) is increased by 25% and Blue has won. Blue remains136-strong.

In the second graph, because the Infection Spread Rate σ (sigma) is increased, when it is compared to base case, the system is affected more (roughly 640) by the malware.

**Case 7;** The variables are presented below. The Kinetic Attack Rate of Blue δ (delta) is increased by 1.86%. Other variables are the same with base case.

| **Kinetic Attack Rate of Blue δ (delta)** | **Kinetic Attack Rate of Red γ (gamma)** | **Infection Spread Rate σ (sigma)** | **Infection Removed Rate η (eta)** | **Attack Efficiency Rate λ (lambda)** |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.05093 | 0.052371 | 0.0005 | 0.0003 | 0.25 |

Table 10: Table of Rates



Graphic 8: Graph of Results and Malware Spread

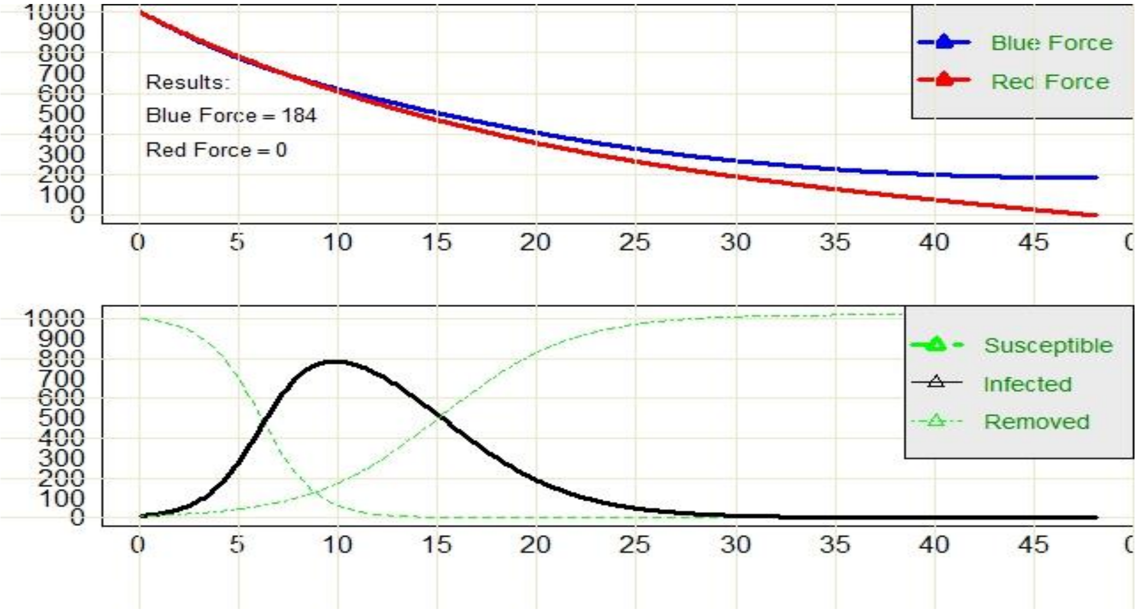
In the first graph, the Kinetic Attack Rate of Blue δ (delta) variable is increased by 1.86%. The Kinetic Attack Rate of Red γ (gamma) and the Infection Spread Rate σ (sigma) is the same with the base case. The 25% increase in the Infection Spread Rate σ (sigma) variable and 1.86% increase in the Kinetic Attack Rate of Blue δ (delta) variable makes the same effect. Blue has won. Blue remains 136-strong.

In the second graph, because the Infection Spread Rate σ (sigma) and the Infection Removed Rate η (eta) is the same with base case, there was no change. Malware infected the system (roughly 520) and later on eradicated.

**Case 8;** The variables are presented below. The Infection Spread Reta σ (sigma) is increased by 50%. Other variables are the same with base case.

| **Kinetic Attack Rate of Blue δ (delta)** | **Kinetic Attack Rate of Red γ (gamma)** | **Infection Spread Rate σ (sigma)** | **Infection Removed Rate η (eta)** | **Attack Efficiency Rate λ (lambda)** |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.052371 | 0.000750 | 0.0003 | 0.25 |

Table 11: Table of Rates



Graphic 9: Graph of Results and Malware Spread

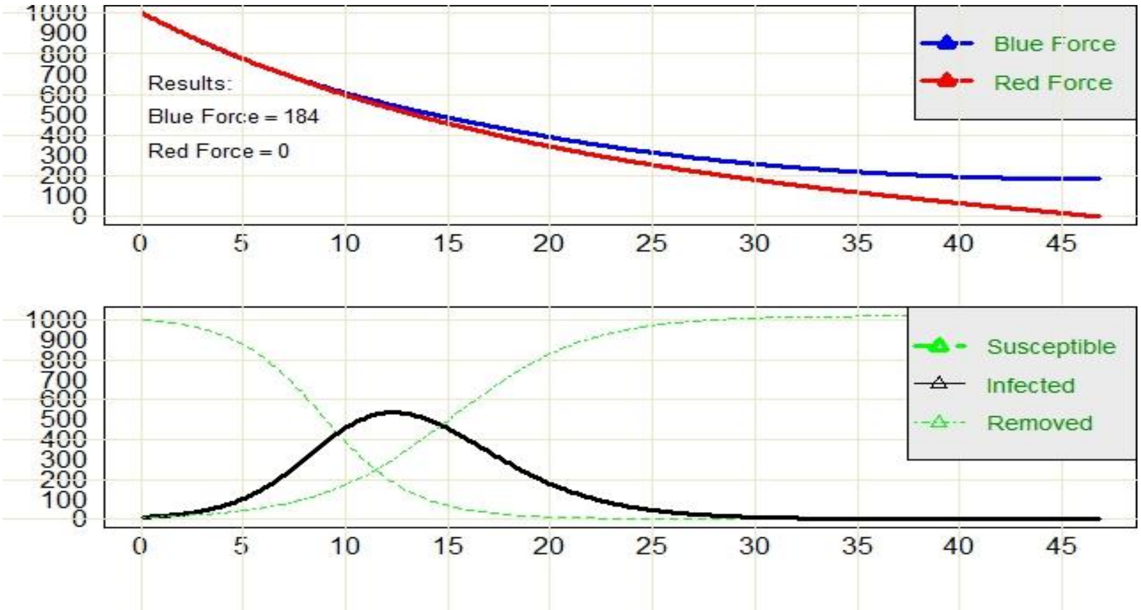
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are the same with the base case. The Infection Spread Rate σ (sigma) is increased by 50% and Blue has won. Blue remains184-strong.

In the second graph, because the Infection Spread Rate σ (sigma) is increased, when it is compared to base case, the system is affected more (roughly 800) by the malware.

**Case 9;** The variables are presented below. Kinetic Attack Rate of Blue δ (delta) is increased by 3.44%. Other variables are the same with base case.

| **Kinetic Attack Rate of Blue δ (delta)** | **Kinetic Attack Rate of Red γ (gamma)** | **Infection Spread Rate σ (sigma)** | **Infection Removed Rate η (eta)** | **Attack Efficiency Rate λ (lambda)** |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.05172 | 0.052371 | 0.0005 | 0.0003 | 0.25 |

Table 12: Table of Rates



Graphic 10: Graph of Results and Malware Spread

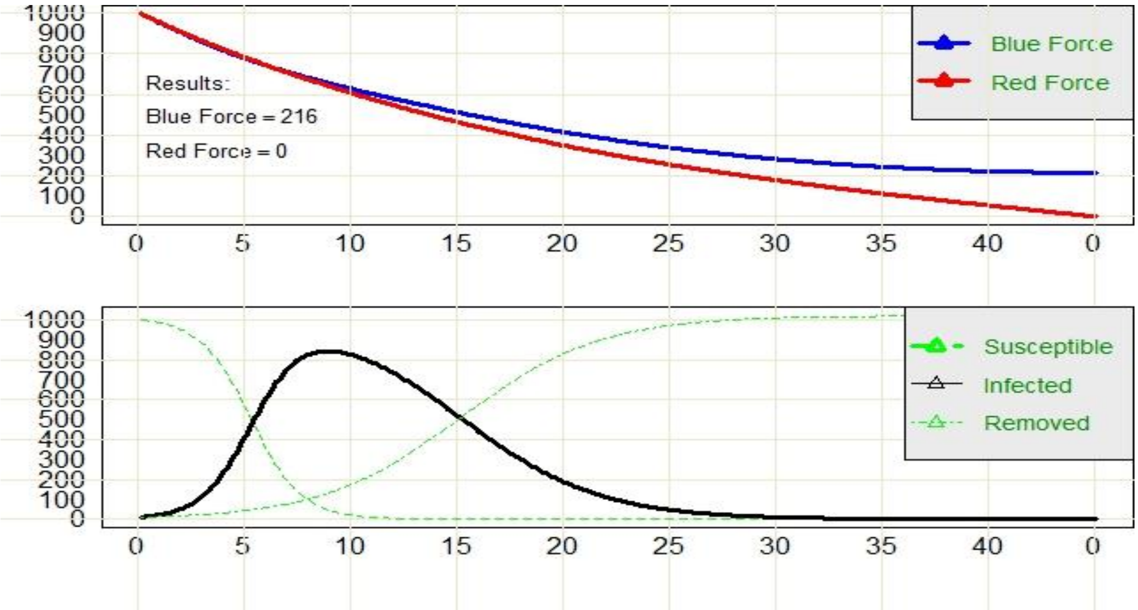
In the first graph, the Kinetic Attack Rate of Blue δ (delta) variable is increased by 3.44%. The Kinetic Attack Rate of Red γ (gamma) and the Infection Spread Rate σ (sigma) is the same with the base case. The 50% increase in the Infection Spread Rate σ (sigma) variable and 3.44% increase in the Kinetic Attack Rate of Blue δ (delta) variable have the same effect. Blue has won. Blue remains 184-strong.

In the second graph, because the Infection Spread Rate σ (sigma) and the Infection Removed Rate η (eta) is the same with base case, there was no change. Malware infected the system (roughly 520) and later on eradicated.

**Case 10;** The variables are presented below. The Infection Spread Reta σ (sigma) is increased by 75%. Other variables are the same with base case.

| Kinetic Attack Rate of Blue δ (delta) | Kinetic Attack Rate of Red γ (gamma) | Infection Spread Rate σ (sigma) | Infection Removed Rate η (eta) | Attack Efficiency Rate λ (lambda) |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.052371 | 0.000875 | 0.0003 | 0.25 |

Table 13: Table of Rates



Graphic 11: Graph of Results and Malware Spread

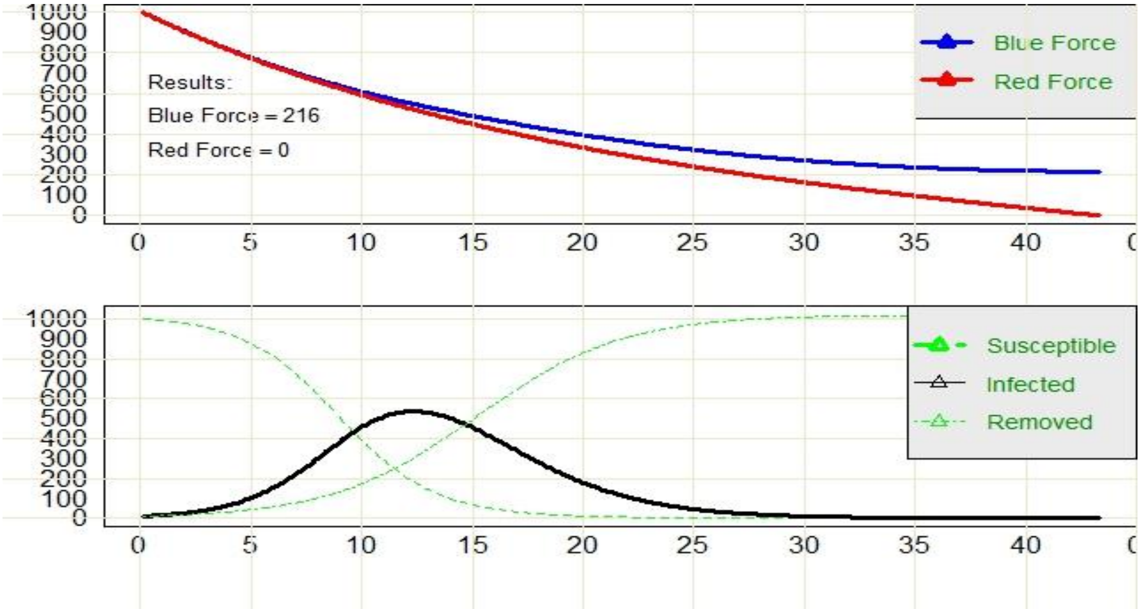
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are the same with the base case. The Infection Spread Rate σ (sigma) is increased by 75% and Blue has won. Blue remains216-strong.

In the second graph, because the Infection Spread Rate σ (sigma) is increased, when it is compared to base case, the system is affected more (roughly 820) by the malware.

**Case 11;** The variables are presented below. The Kinetic Attack Rate of Blue δ (delta) is increased by 4.82%. Other variables are the same with base case.

| **Kinetic Attack Rate of Blue δ (delta)** | **Kinetic Attack Rate of Red γ (gamma)** | **Infection Spread Rate σ (sigma)** | **Infection Removed Rate η (eta)** | **Attack Efficiency Rate λ (lambda)** |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.05241 | 0.052371 | 0.0005 | 0.0003 | 0.25 |

Table 14: Table of Rates



Graphic 12: Graph of Results and Malware Spread

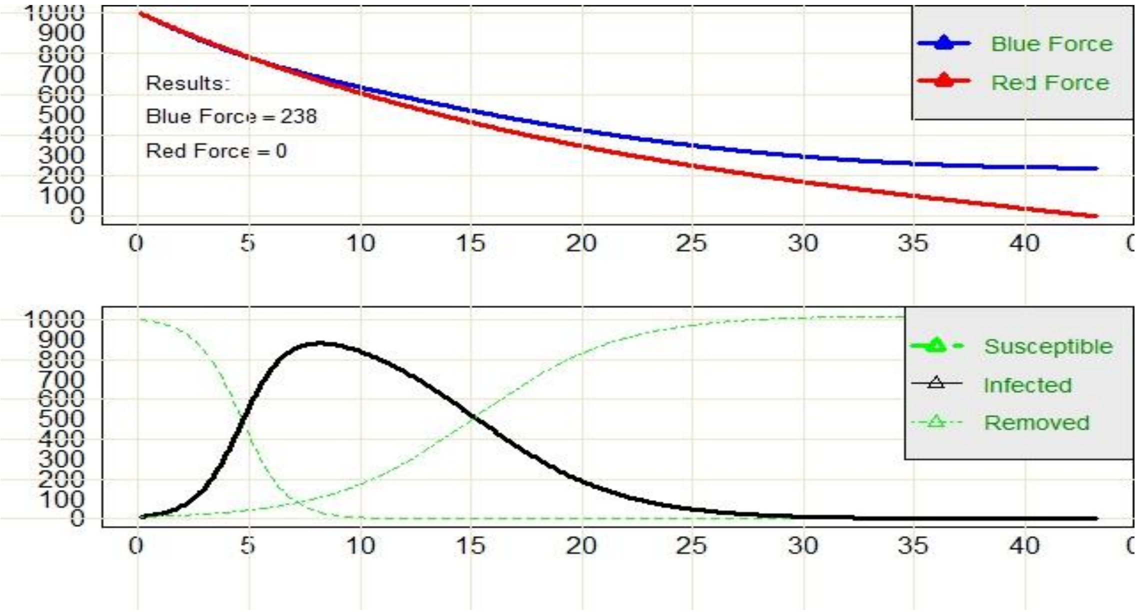
In the first graph, the Kinetic Attack Rate of Blue δ (delta) variable is increased by 4.82%. The Infection Spread Rate σ (sigma) variable is the same with the base case. The 75 % increase in the Infection Spread Rate σ (sigma) variable and 4.82% increase in the Kinetic Attack Rate of Blue δ (delta) variable makes the same effect. Blue has won. Blue remains 216-strong.

In the second graph, because the Infection Spread Rate σ (sigma) and the Infection Removed Rate η (eta) is the same with base case, there was no change. Malware infected the system (roughly 520) and later on eradicated.

**Case 12;** The variables are presented below. The Infection Spread Reta σ (sigma) is increased by 100%. Other variables are the same with base case.

| Kinetic Attack Rate of Blue δ (delta) | Kinetic Attack Rate of Red γ (gamma) | Infection Spread Rate σ (sigma) | Infection Removed Rate η (eta) | Attack Efficiency Rate λ (lambda) |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.052371 | 0.001 | 0.0003 | 0.25 |

Table 15: Table of Rates



Graphic 13: Graph of Results and Malware Spread

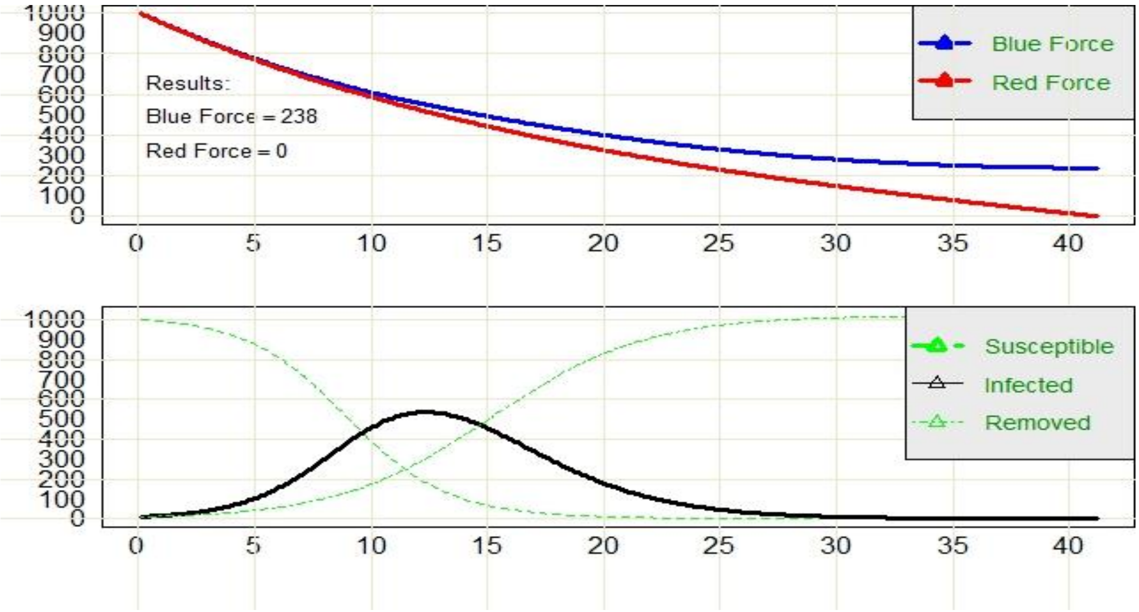
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are the same with the base case. The Infection Spread Rate σ (sigma) is increased by 100% and Blue has won. Blue remains238-strong.

In the second graph, because the Infection Spread Rate σ (sigma) is increased, when it is compared to base case, the system is affected more (roughly 860) by the malware.

**Case 13;** The variables are presented below. The Kinetic Attack Rate of Blue δ (delta) is increased by 5.90%. Other variables are the same with base case.

| **Kinetic Attack Rate of Blue δ (delta)** | **Kinetic Attack Rate of Red γ (gamma)** | **Infection Spread Rate σ (sigma)** | **Infection Removed Rate η (eta)** | **Attack Efficiency Rate λ (lambda)** |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.05295 | 0.052371 | 0.0005 | 0.0003 | 0.25 |

Table 16: Table of Rates



Graphic 14: Graph of Results and Malware Spread

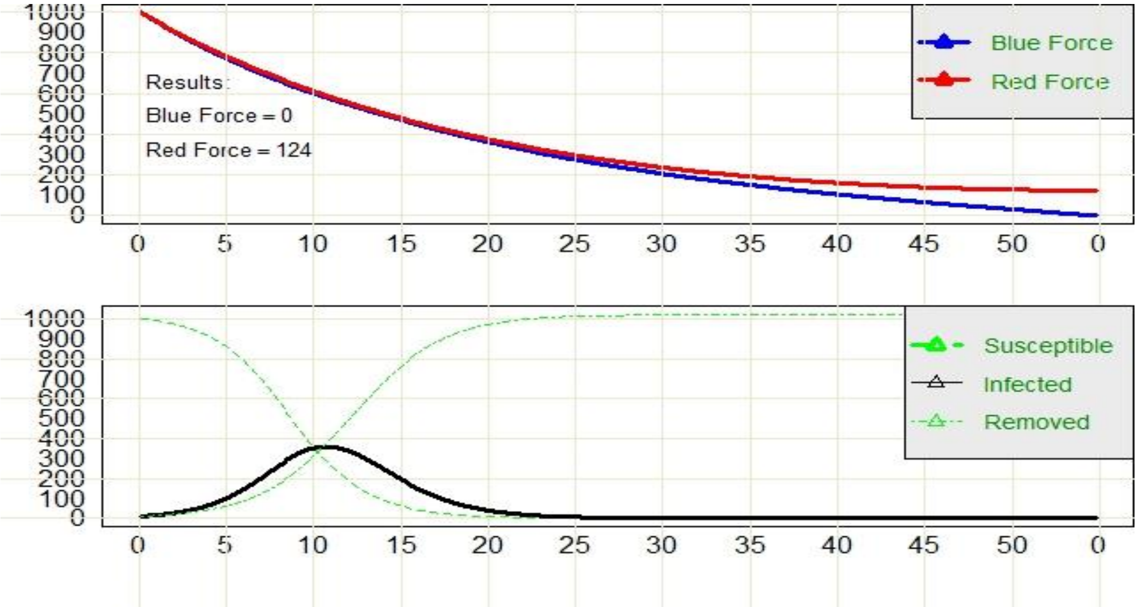
In the first graph, the Kinetic Attack Rate of Blue δ (delta) variable is increased by 5.90%. The Infection Spread Rate σ (sigma) variable is the same with the base case. The 100 % increase in the Infection Spread Rate σ (sigma) variable and 5.90% increase in the Kinetic Attack Rate of Blue δ (delta) variable makes the same effect. Blue has won. Blue remains 238-strong.

In the second graph, because the Infection Spread Rate σ (sigma) and the Infection Removed Rate η (eta) is the same with base case, there was no change. Malware infected the system (roughly 520) and later on eradicated.

**Case 14;** The variables are presented below. The Infection Removed Reta η (eta) is increased by 25%. Other variables are the same with base case.

| **Kinetic Attack Rate of Blue δ (delta)** | **Kinetic Attack Rate of Red γ (gamma)** | **Infection Spread Rate σ (sigma)** | **Infection Removed Rate η (eta)** | **Attack Efficiency Rate λ (lambda)** |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.052371 | 0.0005 | 0.000375 | 0.25 |

Table 17: Table of Rates



Graphic 15: Graph of Results and Malware Spread

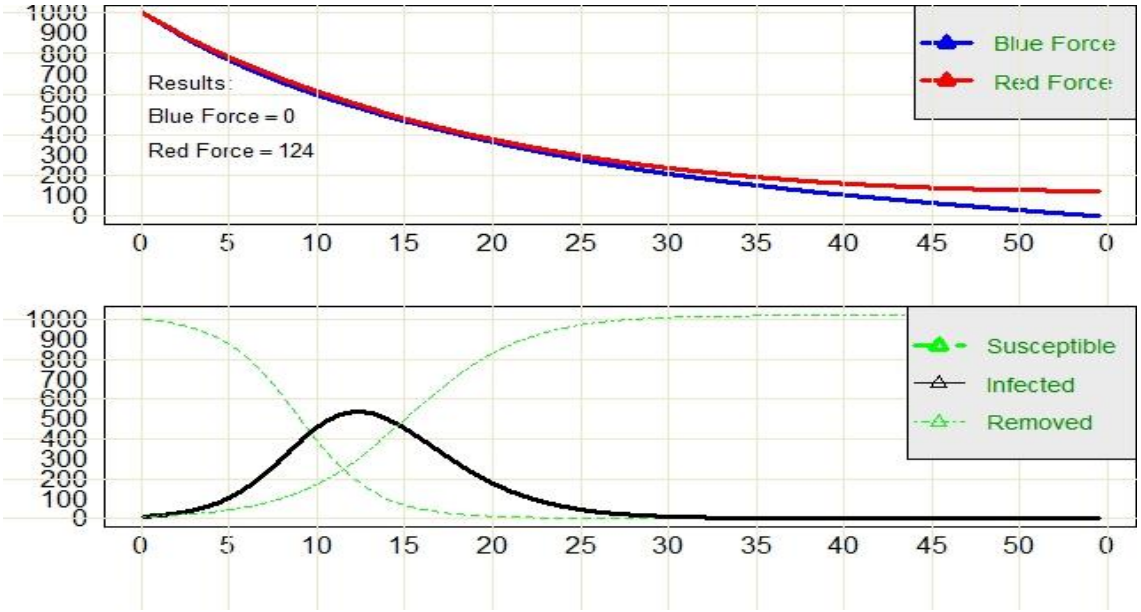
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are the same with the base case. The Infection Removed Reta η (eta) is increased by 25% and Red has won. Red remains 238-strong.

In the second graph, because the Infection Removed Reta η (eta)is increased, when it is compared to base case, the system is affected less (roughly 380) by the malware.

**Case 15;** The variables are presented below. The Kinetic Attack Rate of Red γ (gamma) is increased by 1.60%. Other variables are the same with base case.

| **Kinetic Attack Rate of Blue δ (delta)** | **Kinetic Attack Rate of Red γ (gamma)** | **Infection Spread Rate σ (sigma)** | **Infection Removed Rate η (eta)** | **Attack Efficiency Rate λ (lambda)** |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.053210 | 0.0005 | 0.0003 | 0.25 |

Table 18: Table of Rates



Graphic 16: Graph of Results and Malware Spread

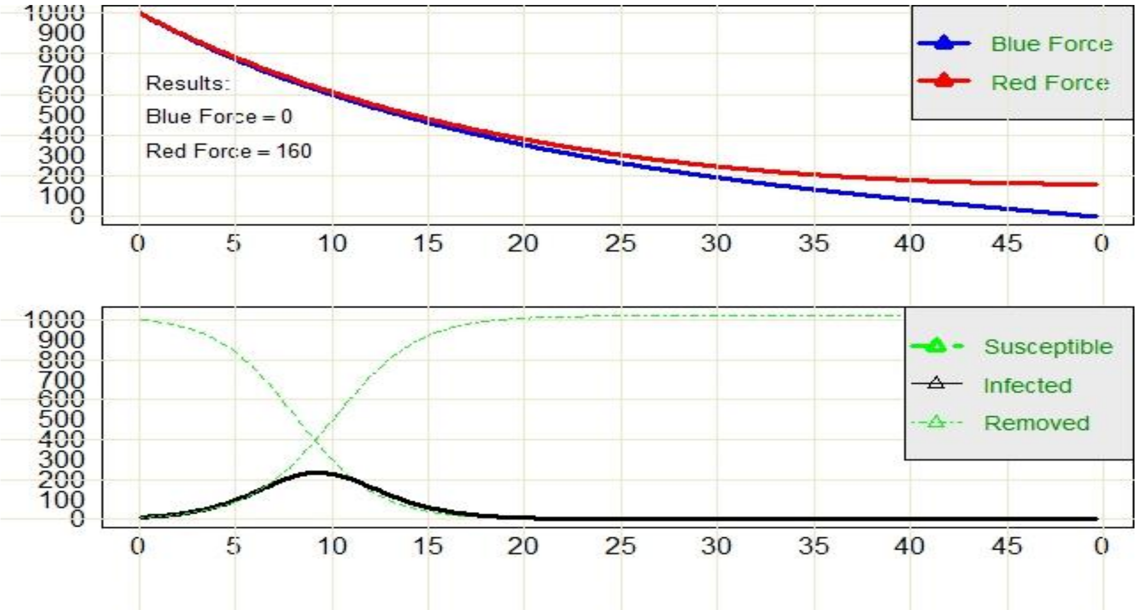
In the first graph, the Kinetic Attack Rate of Red γ (gamma) variable is increased by 1.60%. The Infection Removed Rate η (eta) variable is the same with the base case. The 25 % increase in the Infection Removed Rate η (eta) variable and 1.60% increase in the Kinetic Attack Rate of Red γ (gamma) variable makes the same effect. Red has won. Red remains 124-strong.

In the second graph, because the Infection Spread Rate σ (sigma) and the Infection Removed Rate η (eta) is the same with base case, there was no change. Malware infected the system (roughly 520) and later on eradicated.

**Case 16;** The variables are presented below. The Infection Removed Reta η (eta) is increased by 50%. Other variables are the same with base case.

| Kinetic Attack Rate of Blue δ (delta) | Kinetic Attack Rate of Red γ (gamma) | Infection Spread Rate σ (sigma) | Infection Removed Rate η (eta) | Attack Efficiency Rate λ (lambda) |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.052371 | 0.0005 | 0.000450 | 0.25 |

Table 19: Table of Rates



Graphic 17: Graph of Results and Malware Spread

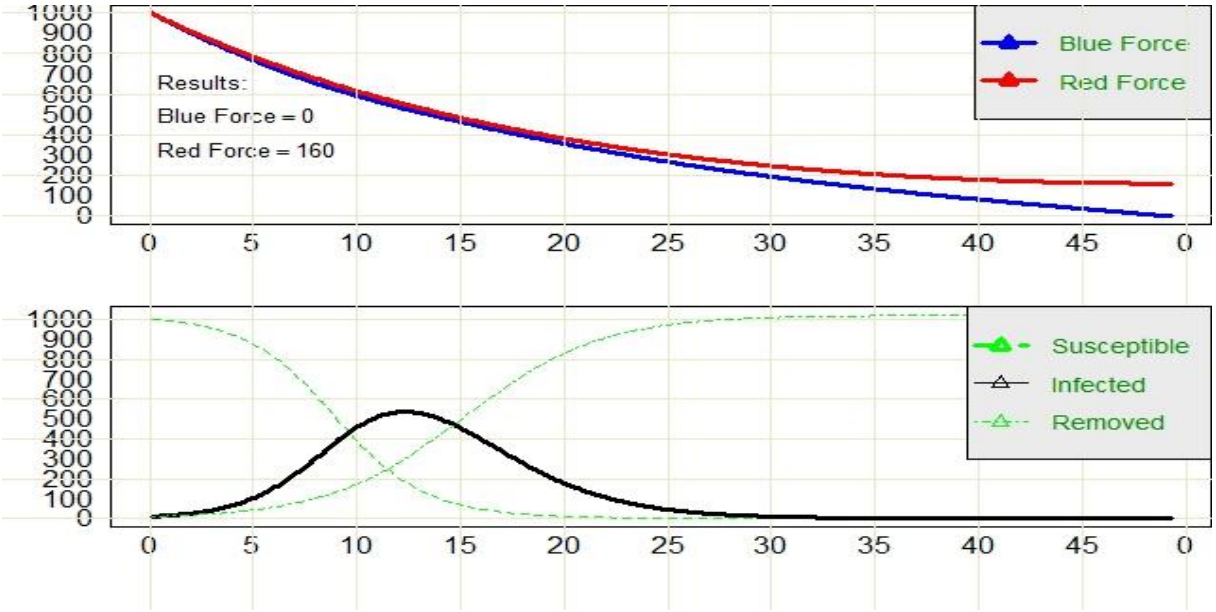
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are the same with the base case. The Infection Removed Reta η (eta) is increased by 50% and Red has won. Red remains 160-strong.

In the second graph, because the Infection Removed Reta η (eta)is increased, when it is compared to base case, the system is affected less (roughly 220) by the malware.

**Case 17;** The variables are presented below. The Kinetic Attack Rate of Red γ (gamma) is increased by 2.69%. Other variables are the same with base case.

| Kinetic Attack Rate of Blue δ (delta) | Kinetic Attack Rate of Red γ (gamma) | Infection Spread Rate σ (sigma) | Infection Removed Rate η (eta) | Attack Efficiency Rate λ (lambda) |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.053782 | 0.0005 | 0.0003 | 0.25 |

Table 20: Table of Rates



Graphic 18: Graph of Results and Malware Spread

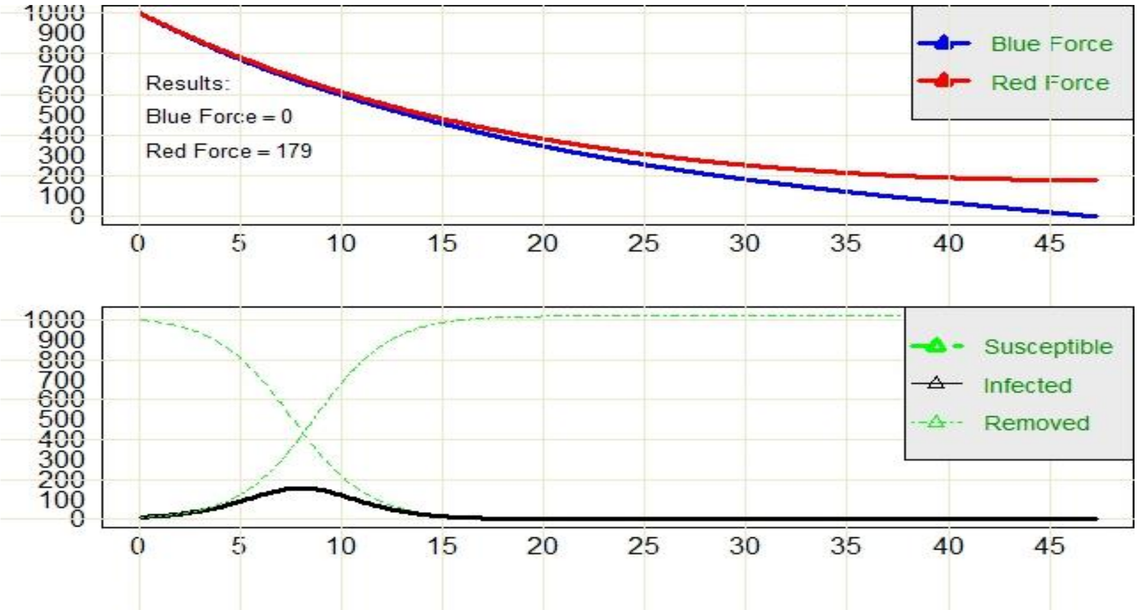
In the first graph, the Kinetic Attack Rate of Red γ (gamma) variable is increased by 2.69%. The Infection Removed Rate η (eta) variable is the same with the base case. The 50 % increase in the Infection Removed Rate η (eta) variable and 2.69% increase in the Kinetic Attack Rate of Red γ (gamma) variable makes the same effect. Red has won. Red remains 160-strong.

In the second graph, because the Infection Spread Rate σ (sigma) and the Infection Removed Rate η (eta) is the same with base case, there was no change. Malware infected the system (roughly 520) and later on eradicated.

**Case 18;** The variables are presented below. The Infection Removed Reta η (eta) is increased by 75%. Other variables are the same with base case.

| Kinetic Attack Rate of Blue δ (delta) | Kinetic Attack Rate of Red γ (gamma) | Infection Spread Rate σ (sigma) | Infection Removed Rate η (eta) | Attack Efficiency Rate λ (lambda) |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.052371 | 0.0005 | 0.000525 | 0.25 |

Table 21: Table of Rates



Graphic 19: Graph of Results and Malware Spread

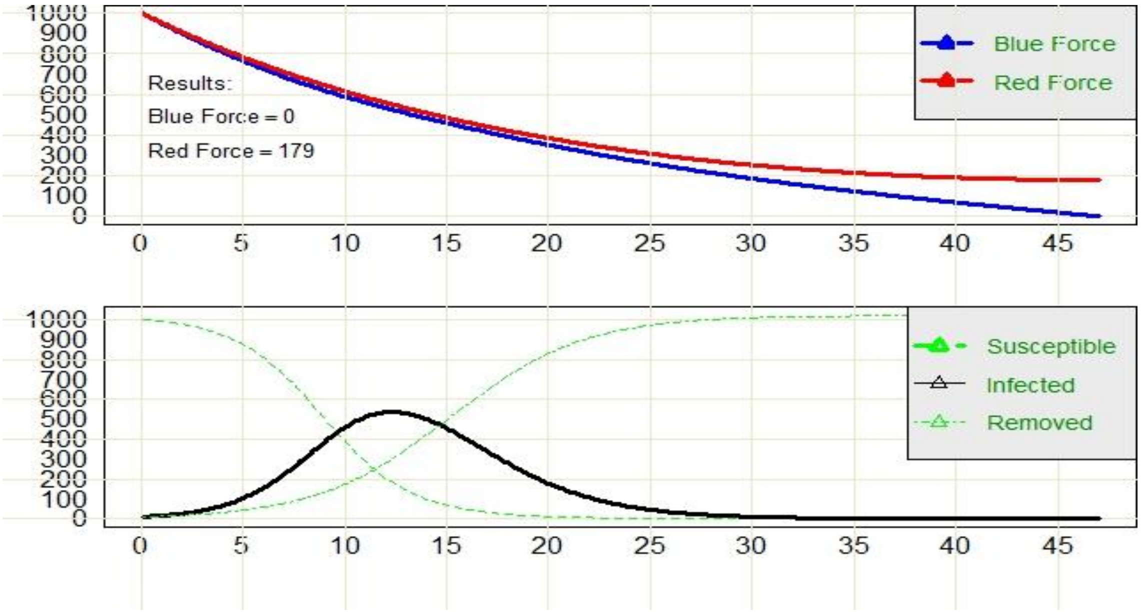
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are the same with the base case. The Infection Removed Reta η (eta) is increased by 75% and Red has won. Red remains 179-strong.

In the second graph, because the Infection Removed Reta η (eta)is increased, when it is compared to base case, the system is affected less (roughly 180) by the malware.

**Case 19;** The variables are presented below. The Kinetic Attack Rate of Red γ (gamma) is increased by 3.35%. Other variables are the same with base case.

| Kinetic Attack Rate of Blue<br>δ (delta) | Kinetic Attack Rate of Red<br>γ (gamma) | Infection Spread Rate<br>σ (sigma) | Infection Removed Rate<br>η (eta) | Attack Efficiency Rate<br>λ (lambda) |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.054129 | 0.0005 | 0.0003 | 0.25 |

Table 22: Table of Rates



Graphic 20: Graph of Results and Malware Spread

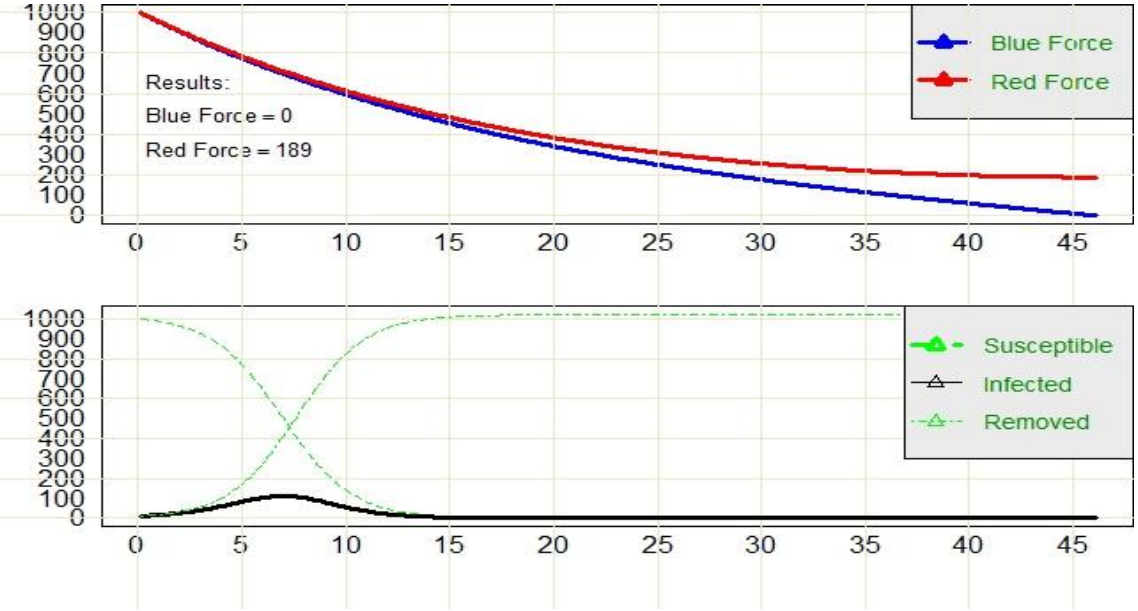
In the first graph, the Kinetic Attack Rate of Red γ (gamma) variable is increased by 3.35%. The Infection Removed Rate η (eta) variable is the same with the base case. The 75% increase in the Infection Removed Rate η (eta) variable and 3.35% increase in the Kinetic Attack Rate of Red γ (gamma) variable makes the same effect. Red has won. Red remains 179-strong.

In the second graph, because the Infection Spread Rate σ (sigma) and the Infection Removed Rate η (eta) is the same with base case, there was no change. Malware infected the system (roughly 520) and later on eradicated.

**Case 20;** The variables are presented below. The Infection Removed Reta η (eta) is increased by 100%. Other variables are the same with base case.

| Kinetic Attack Rate of Blue<br>δ (delta) | Kinetic Attack Rate of Red<br>γ (gamma) | Infection Spread Rate<br>σ (sigma) | Infection Removed Rate<br>η (eta) | Attack Efficiency Rate<br>λ (lambda) |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.052371 | 0.0005 | 0.0006 | 0.25 |

Table 23: Table of Rates



Graphic 21: Graph of Results and Malware Spread

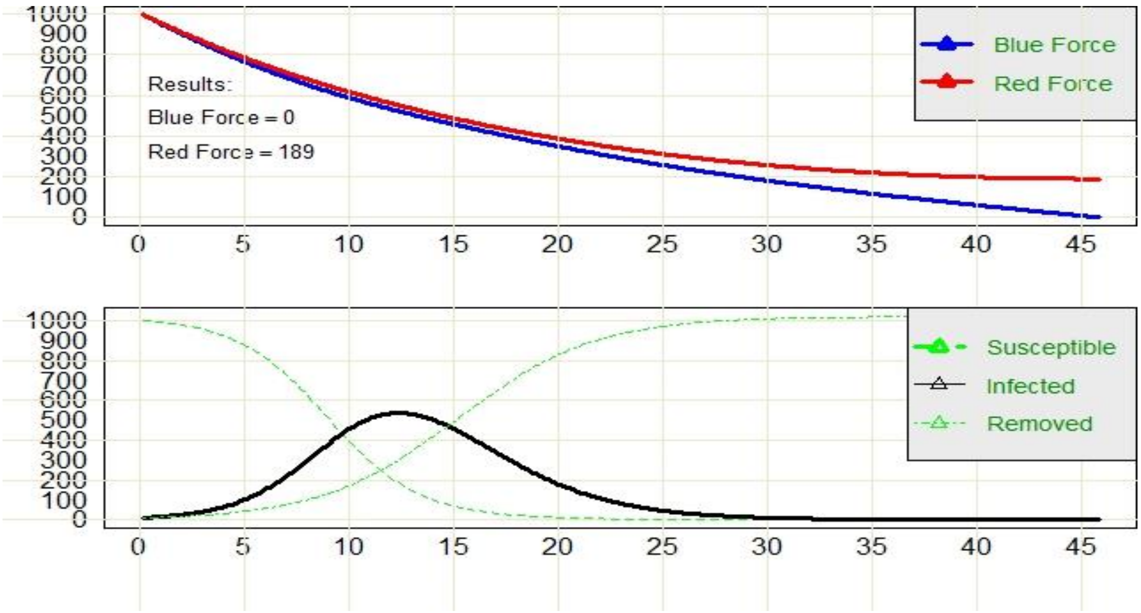
In the first graph, the Kinetic Attack Rate of Blue δ (delta) and the Kinetic Attack Rate of Red γ (gamma) variables are the same with the base case. The Infection Removed Reta η (eta) is increased by 100% and Red has won. Red remains 189-strong.

In the second graph, because the Infection Removed Reta η (eta) is increased, when it is compared to base case, the system is affected less (roughly 110) by the malware.

**Case 21;** The variables are presented below. The Kinetic Attack Rate of Red γ (gamma) is increased by 3.78%. Other variables are the same with base case.

| Kinetic Attack Rate of Blue δ (delta) | Kinetic Attack Rate of Red γ (gamma) | Infection Spread Rate σ (sigma) | Infection Removed Rate η (eta) | Attack Efficiency Rate λ (lambda) |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.054354 | 0.0005 | 0.0003 | 0.25 |

Table 24: Table of Rates



Graphic 22: Graph of Results and Malware Spread

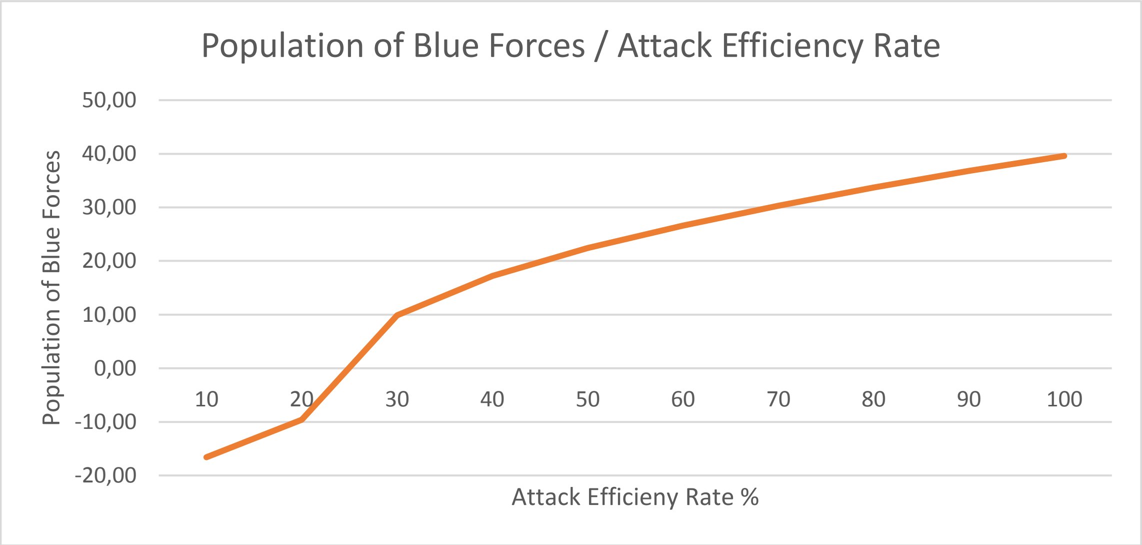
In the first graph, the Kinetic Attack Rate of Red γ (gamma) variable is increased by 3.78%. The Infection Removed Rate η (eta) variable is the same with the base case. The 100% increase in the Infection Removed Rate η (eta) variable and 3.78% increase in the Kinetic Attack Rate of Red γ (gamma) variable makes the same effect. Red has won. Red remains 189-strong.

In the second graph, because the Infection Spread Rate σ (sigma) and the Infection Removed Rate η (eta) is the same with base case, there was no change. Malware infected the system (roughly 520) and later on eradicated.

Attack Efficiency Rate λ (lambda) is increased from 10% to 100% by 10 units and is compared with the base case.

| Kinetic Attack Rate of Blue δ (delta) | Kinetic Attack Rate of Red γ (gamma) | Infection Spread Rate σ (sigma) | Infection Removed Rate η (eta) | Attack Efficiency Rate λ (lambda) |
|---|---|---|---|---|
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 |
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.1 |
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.2 |
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.3 |
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.4 |
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.5 |
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.6 |
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.7 |
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.8 |
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.9 |
| 0.050 | 0.052371 | 0.0005 | 0.0003 | 1.0 |

Table 25: Table of Attack Efficiency Rates



Graphic 23: Graph of Attack Efficiency Rate Effects

In base case where both sides cannot have superiority on each other, Red wins when Attack Efficiency rate is lower than 25%, and Blue wins when Attack Efficiency Rate is higher than 25%

# CHAPTER 5

# DISCUSSION AND FUTURE WORK

## 5.1. Discussion

This thesis aimed at to contributing to our understanding of how a cyber attack could affect a kinetic battle. Mathematical models and simulations were designed to give a general idea to understand and identify parts of an up to date phenomenon. The findings were obtained within the framework of the assumptions and the limitations  of the background models.

The proposed model and its analyses revealed that war in cyber space, which was implemented as a DDoS attack in this thesis work, has potential to have an impact on a kinetic battle. This finding is based on a set of assumptions, which state that the fighting sides employ cyber systems, they may be influenced by bandwidth saturation, and  the bandwidth saturation can be provided by the processing power that is fetched from the white population computers by means of malware injection. The results indicate that depending on the effectiveness of the specific cyber attack and how it affects the target, a  cyber attack has potential to be used as a game changer for a kinetic battle. The results are shown in Table 26.

| **Case** | **Kinetic Attack Rate of Blue δ (delta)** | **Kinetic Attack Rate of Red γ (gamma)** | **Infection Spread Rate σ (sigma)** | **Infection Removed Rate η (eta)** | **Attack Efficiency Rate λ (lambda)** | **Explanation** | **Winner** | **Winner Population End of the Battle** |
|---|---|---|---|---|---|---|---|---|
| 1 | 0.050 | 0.050 | 0.00 | 0.00 | 0.00 | - | None | 18-18 |
| 2 | 0.050 | 0.050 | 0.0005 | 0.0005 | 0.00 | - | None | 18-18 |
| 3 | 0.050 | 0.050 | 0.0005 | 0.0003 | 0.00 | - | None | 18-18 |
| 4 | 0.050 | 0.050 | 0.0005 | 0.0003 | 0.25 | - | Blue | 215 |
| 5 | 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.25 | Base Case | None | 17-17 |
| Kinetic Attack Rate of Blue and Infection Spread Rate | | | | | | | | |
| 6 | 0.050 | 0.052371 | 0.000625 | 0.0003 | 0.25 | +25% | Blue | 136 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 7 | 0.05093 | 0.052371 | 0.0005 | 0.0003 | 0.25 | +1,86% | Blue | 136 |
| 8 | 0.050 | 0.052371 | 0.000750 | 0.0003 | 0.25 | +50% | Blue | 184 |
| 9 | 0.05172 | 0.052371 | 0.0005 | 0.0003 | 0.25 | +3,44% | Blue | 184 |
| 10 | 0.050 | 0.052371 | 0.000875 | 0.0003 | 0.25 | +75% | Blue | 216 |
| 11 | 0.05241 | 0.052371 | 0.0005 | 0.0003 | 0.25 | +4,82% | Blue | 216 |
| 12 | 0.050 | 0.052371 | 0.001 | 0.0003 | 0.25 | +100% | Blue | 238 |
| 13 | 0.05295 | 0.052371 | 0.0005 | 0.0003 | 0.25 | +5,90% | Blue | 238 |
| Kinetic Attack Rate of Red and Infection Removed Rate | | | | | | | | |
| 14 | 0.050 | 0.052371 | 0.0005 | 0.000375 | 0.25 | +25% | Red | 124 |
| 15 | 0.050 | 0.053210 | 0.0005 | 0.0003 | 0.25 | +1,60% | Red | 124 |
| 16 | 0.050 | 0.052371 | 0.0005 | 0.000450 | 0.25 | +50% | Red | 160 |
| 17 | 0.050 | 0.053782 | 0.0005 | 0.0003 | 0.25 | +2,69% | Red | 160 |
| 18 | 0.050 | 0.052371 | 0.0005 | 0.000525 | 0.25 | +75% | Red | 179 |
| 19 | 0.050 | 0.054129 | 0.0005 | 0.0003 | 0.25 | +3,35% | Red | 179 |
| 20 | 0.050 | 0.052371 | 0.0005 | 0.0006 | 0.25 | +100% | Red | 189 |
| 21 | 0.050 | 0.054354 | 0.0005 | 0.0003 | 0.25 | +3,78% | Red | 189 |
| Attack Efficiency Rate | | | | | | | | |
| | 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.1 | 10% | Red | 166 |
| | 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.2 | 20% | Red | 96 |
| | 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.3 | 30% | Blue | 99 |
| | 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.4 | 40% | Blue | 172 |
| | 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.5 | 50% | Blue | 224 |
| | 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.6 | 60% | Blue | 266 |
| | 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.7 | 70% | Blue | 303 |
| | 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.8 | 80% | Blue | 337 |
| | 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.9 | 90% | Blue | 368 |
| | 0.050 | 0.052371 | 0.0005 | 0.0003 | 0.10 | 100% | Blue | 396 |

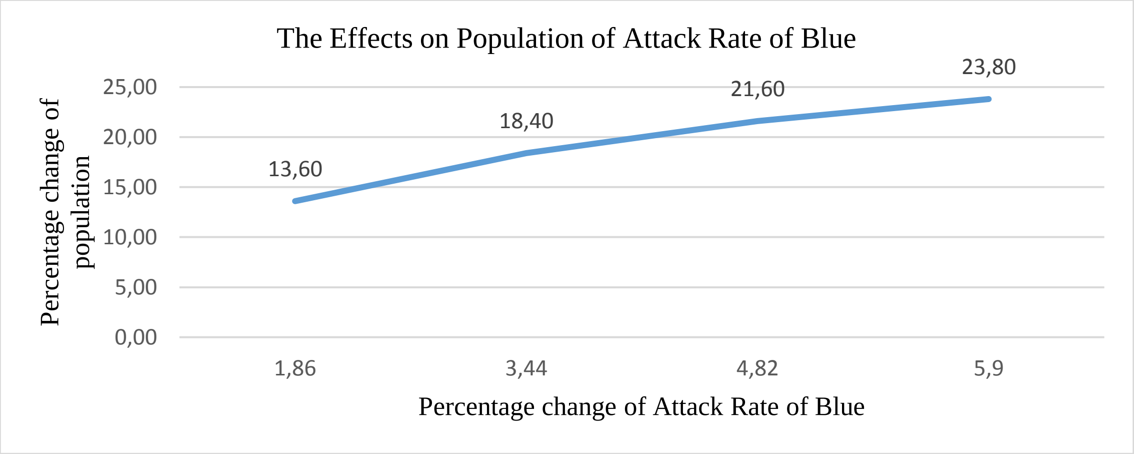
Table 26: All variables and Results Table (Advantages of Blue; Kinetic Attack Rate of Blue δ (delta); Infection Spread Rate σ (sigma); Attack Efficiency Rate λ (lambda); Advantages of Red; Kinetic Attack Rate of Red γ (gamma); Infection Removed Rate η (eta)).

According to the findings presented in the table, both 1.86% increase in the Blue forces or 25% increase in the Infection Spread Rate result in similar effects. Blue wins the war and the Blue forces remain 136-strong out of 1000. Similarly, a 3.44% increase in the Blue forces or a 50% increase in the Infection Spread Rate lead to similar effects; Blue wins the war and Blue forces remain 184-strong out of 1000. A 4.86% increase in the Blue forces or a 75% increase in the Infection Spread Rate lead to similar effects, as well; Blue wins the war and Blue forces remain 216-strong out of 1000. Finally, a 5.90% increase in the Blue forces or a 100% increase in the Infection Spread Rate makes the same effects; Blue wins the war and Blue forces remain 136-strong out of 1000.

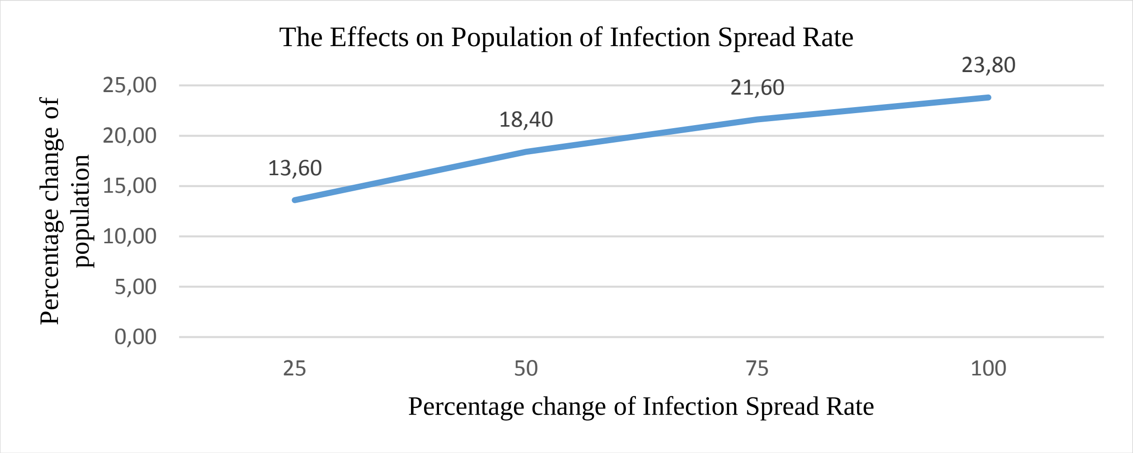
Table 27 shows the effects on population when there is a change in the Blue Force variables. Graphic 24 and 25 show the effects of the Attack Rate and the Infection Spread Rate of the Blue forces, respectively.

| | **Exchange Ratio** | | | |
|---|---|---|---|---|
| Percentage (%) change of Kinetic Attack Rate | 1.86 | 3.44 | 4.82 | 5.90 |
| Percentage (%) change of Infection Spread Rate | 25 | 50 | 75 | 100 |
| The percentage (%) change of Blue survivors when all variables are applied one by one | 13.60 | 18.40 | 21.60 | 23.80 |

Table 27 The effects on population when there is a change in Blue force variables



Graphic 24: The Effects on Population of Attack Rate of Blue



Graphic 25: The Effects of Population of Infection Spread Rate

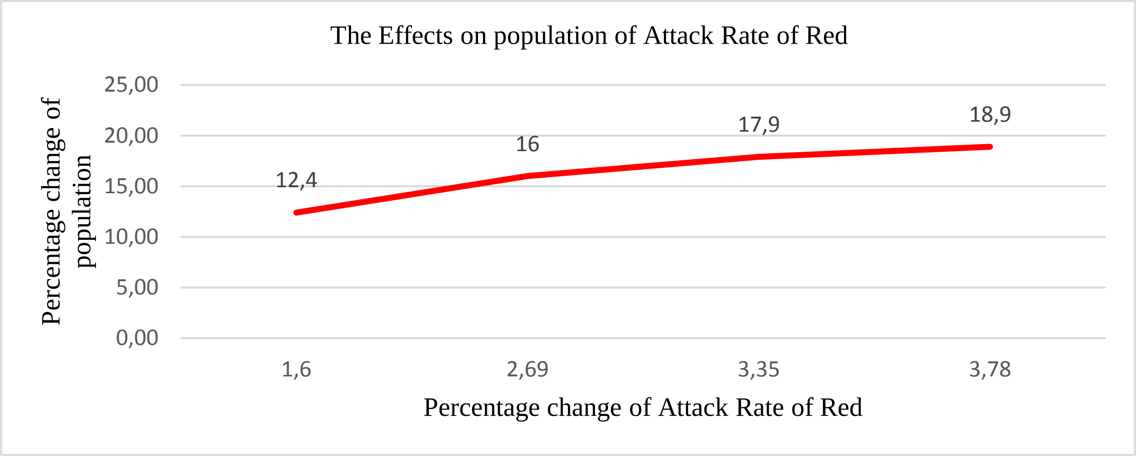
Based on he framework assumptions; the results show that a 1.6% increase in Red forces or a 25% increase in the Infection Spread Rate leads to similar effects. The Red wins the war and the Red forces remain 124-strong out of 1000. Similarly, a 2.69% increase in the Red forces or a 50% increase in the Infection Spread Rate leads to similar effects. The Red wins the war and the Red forces remain 160-strong out of 1000. A 3.35% increase in the Red forces or a 75% increase in the Infection Spread Rate results in similar effects. The Red wins the war and the Red forces remain 179-strong out of 1000. Finally, a 3.78% increase in the Red forces or a 100% increase in the Infection Spread Rate leads to similar effects. The Red wins the war and the Red forces remain 189-strong out of 1000.

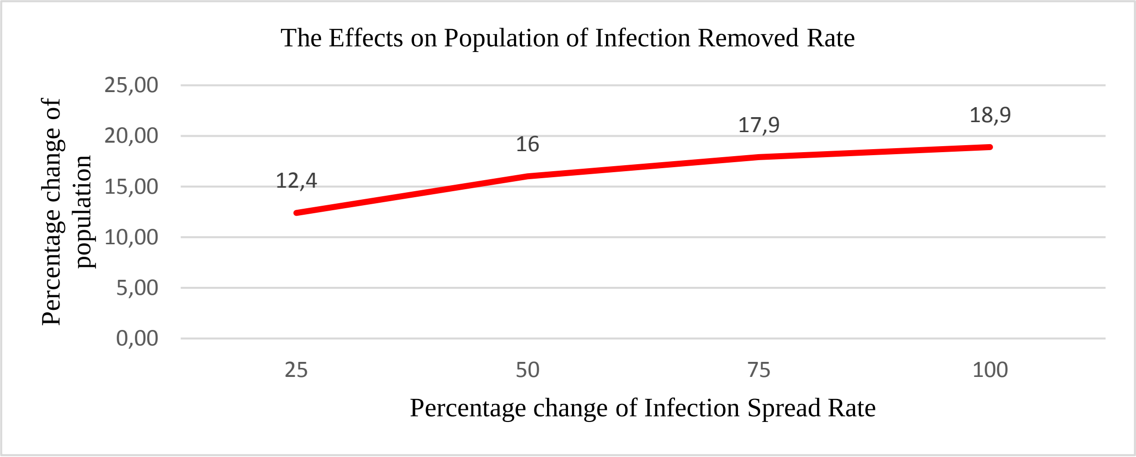
Table 28 shows the effects on population when there is a change in the Red Force variables . Graphic 26 and Graphic 27 show the effects of the Attack Rate and the Infection Removed Rate on the Red forces, respectively.

| | **Exchange Ratio** | | | |
|---|---|---|---|---|
| Percentage (%) change of Kinetic Attack Rate of Red | 1.6 | 2.69 | 3.35 | 3.78 |
| Percentage (%) change of Infection Removed Rate | 25 | 50 | 75 | 100 |
| The percentage (%) change of Red survivors when all variables are applied one by one | 12.4 | 16 | 17.9 | 18.9 |

Table 28: The effects on population when there is a change in Red force variables

Graphic 26: The Effects on Population of Attack Rate of Red





Graphic 27: The effects on Population of Infection Removed Rate

Based on the results of the proposed model, cyber war capability has been shown to be a factor that has potential to influence the outcomes of a war, both in terms of offense and defense. In terms of offense, the marginal benefits of increasing the cyber war capabilities and the offense capabilities of the armed forces gradually decrease. In terms of defense, the marginal benefits of increasing the cyber war capabilities and the offense capabilities of the armed forces gradually decrease, as well. In case of a real-world scenario, by creating a similar model and adding costs of war into it, it may be possible to make assumptions on what capabilities to increase or what should be done in order to get optimal results.

A major assumption in the thesis was that only the Blue Forces were able to install malware in White forces' computers. The malware was installed in the White's computers before the war begins, and it started to spread and initiated DDoS attacks. Accordingly, our results showed that if the Blue Forces could spread malware to more computers before the war begins, the Blue Forces were able to win the war more easily. If the Blue Forces initiated DDoS attacks, the malware could be detected earlier and eradicated in a short time span. Initially, the malware installed at a computer can wait in ambush, spreading to more than one computer without initiating DDoS attacks. With the beginning of the war, malware that had spread to more computers can initiate DDoS attacks. Thus, the Red Forces could be eliminated in a shorter time.

The Area-fire model (aka. the Linear Model) and the Aimed-fire model (aka. the Square Model), as subtypes of the Lanchester Combat (Kinetic) Model, are designated for different tasks. The Linear model was a more appropriate selection in our case because DDoS attacks are in massive form. In the scenarios that we proposed, a non- direct attack format that limited communication channels was applied. Nevertheless, as mentioned previously, the Blue Forces' scope for running DDoS attacks are limited to injection to the White Force computers. From that point on, the virus spread and attacked the Red Forces. Meanwhile, the Blue Forces just focused on the physical war. In the scenario, we assumed that the Blue Forces did not make constant injections or they did not design make aimed attacks.

We can conclude that, a DDoS attack can be an effective tool for a kinetic battle. Depending on the effectiveness of the DDoS attack, and how it affects the target, at some point it can be used as a game changer.

## 5.2. Future Work

The future research should address designing an Aimed-fire Lanchester Model, the addition of ambush modification to the model and making scenarios out of these circumstances. It should also focus on an analysis of real-world scenarios and data. Economical models that address the cost considerations might enrich the modelling perspective presented in this thesis.

The model was generated with limited parameters, but the analyses can be expanded on further parameters, such as infiltration rates, ADS types, or viral infection spread types. In this model scenario, the selection of the White population and their connection bandwidth capacity, the effectiveness specification of the virus, the communication dependence of the Red forces, and other relevant measures that characterize a DDoS attack also have potential to affect the Red Forces, which should be addressed by future research.

Another major assumption in the thesis was that each computer was assumed to be connected to a certain number of other computers. However, in a real world scenario, the  computers that are connected to the others may have different topologies. If the number of malware-installed computers is small, then the spreading speed of malware may also be small. However, if the malware-installed computer is connected to a large number of computers, then the spreading speed of the malware may be high. Accordingly, the number of other computers connected to malware-installed computers is a factor that may have significant impact on the results. Therefeore, in future studies, the change of the spreading speed in malware should be taken into consideration. This model can be formulated by adjusting the probability rates (e.g., Pastor-Satomas and Vespignani, 2002).

## REFERENCES

Andress, J., Winterfeld, S. 2012. Cyberwarfare: Techniques, Tactics and Tools for Security Practitioners. Second Edition, Elsevier Press.

Bach, E.R., Dolansky, L. & Stubbs, L.H. 1962. Some Recent Contributions to the Lanchester Theory of Combat. Operations Research, Vol.10:Issue.3: pages. 314-326.

Carr, J. 2011. Inside cyber warfare: Mapping the cyber underworld. O'Reilly, Second Edition. ISBN: 978-1-449-31004-2

Chen, M.T. 2010. Stuxnet, the Real Start of Cyber Warfare? IEEE Network, The Magazine of Global Internetworking. pp.1-3.

Carl von Clausewitz, *On War*, (edited and translated by Michael Howard and Peter Paret), Princeton University Press, 1989, p. 89.

Deitchman, S.J. 1962. A Lanchester Model of Guerrilla Warfare. Operations Research, Vol.10:Issue.6: pages. 818-827.

Department of Defense Dictionary of Military and Associated Terms, 2010. www.dtic.mil/doctrine/new_pubs/dictionary (p.58).

Engel, J. H., 1954. A verification of Lanchester's law. Journal of the Operations Research Society of America 2 163–171.

Erickson, M.G. 1985. A Model of Advertising Competition. Journal of Marketing Research, Vol.22, No.3, pp. 297-304.

Garber, L. 2000. Denial of Service attacks rip the web. IEEE pc, 33,4:12-17.

Gonsalves, C. (2004, June). Akamai DDoS attack whacks Web traffic. Available at http://www.eweek.com/article2/0,1895,1612739,00.asp

Gupta, B.B., Joshi, R.C. & Misra, M. 2009. Defending against Distributed Denial of Service Attacks: Issues and Challenges, Information Security Journal: A Global Perspective, 18:5, 224-247, DOI: 10.1080/19393550903317070

Junio, J.T. 2013. How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate, Journal of Strategic Studies, 36:1, 125-133.

Kermack, W., A. McKendrick. 1927. Contributions to the mathematical theory of epidemics—I. Bulletin of Mathematical Biology (1991) 53(1–2), 33–55.

Kim, D., Moon, H., Park, D., & Shin, H. 2017. An efficient approximate solution for stochastic Lanchester models. Journal of the Operational Research Society. Volume 68, Issue 11, pp. 1470-1481.

Kimball, E.G. 1957. Some Industrial Applications of Military Operations Research Methods. Operations Research, Vol.5:Issue.2: pages. 201-204.

Lanchester, F. W. 1916. Aircraft in warfare: the dawn of the fourth arm. Constable limited, Appleton, NY.

Leiner, B.M., Cerf, V.G., et. al. (2003). *A brief history of the Internet*. Internet Society. Available at http://www.isoc.org

Lindsay,J. R. 2013. Stuxnet and the Limit of Cyber Warfare. Security Studies, 22:3, 365-404.

Little, D.C.J. 1979. Aggregate Advertising Models: The State of the Art. Operations Research, Vol.27:Issue.4: pages. 629-667.McGraw, L., 2013. Cyber War is Inevitable (Unless We Build security In). Journal of Strategic Studies, 36:1, 109-119.

McLaughlin, L.K. 2011. Cyber Attack Is a Counter Attack Warranted?, Information Security Journal: A Global Perspective, 20:1, 58-64

Mirkovic, J. And Reiher, P. 2004. A taxonomy of DDoS attack and DDoS defense mechanisms, SIGCOMM Comput.Commun.REv.34, pp. 39-53.

Molsa, J. 2005. Mitigating denial of service attacks: A tutorial. *Journal of Computer Security*, 13, 807–837.

Murray, J. D. 2002. Mathematical Biology I: An Introduction, vol. 17 of Interdisciplinary Applied Mathematics. Springer, New York, NY.

Ophardt, J.A. 2010. Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow’s battlefield. Duke Law & Technology Review, HeinOnline.

Pastor-Statomas, R., Vespignani, A. (2002) Epidemic Dynamics in Finite Scale-Free Networks. Physical Review E 65

Schramm, H. C., & Gaver, D. P. (2013). Lanchester for cyber: The mixed epidemic combat model. Naval Research Logistics (NRL), 60(7), 599–605.

Singleton, T. 2006. Managing Distributed Denial-Of-Service Attacks, EDPACS, 30:5, 7-20, DOI: 10.1201/1079/43288.30.5.20021101/39237.2

Thiruvaazhi, U. & Alex, M.E. 2012. A Forensic Mechanism to Trace the Master of Distributed Denial-of-Service Attack, Information Security Journal: A Global Perspective, 21:1, 36-46, DOI: 10.1080/19393555.2011.629339

Whittaker, D.J. 2004. Terrorists and terrorism: In the contemporary world. Taylor and Francis e-Library ISBN 0-203-00382-9

Wiener, Norbert. Cybernetics or Control and Communication in the Animal and the Machine, Massachusettsvnstitute of Technology (MIT) press, 1948.

Zaroo, P. (2002). A survey of DDoS attacks and some DDoS defense mechanisms. Technical Report. Lectures Notes for Advanced Information Assurance (CS626), Computer Science Department, Purdue University.

# TEZ FOTOKOPİ İZİN FORMU

**ENSTİTÜ**

Fen Bilimleri Enstitüsü □

Sosyal Bilimler Enstitüsü □

Uygulamalı Matematik Enstitüsü □

Enformatik Enstitüsü ☒

Deniz Bilimleri Enstitüsü □

**YAZARIN**

Soyadı : KILIÇ

Adı : Lütfi

Bölümü : Bilişim Sistemleri

**TEZİN ADI**

Effects of a DDoS Attack on a Mılıtary Operatıon

**TEZİN TÜRÜ** Yüksek Lisans ☒ Doktora □

1. Tezimin tamamı dünya çapında erişime açılsın ve kaynak gösterilmek şartıyla tezimin bir kısmı veya tamamının fotokopisi alınsın. □

2. Tezimin tamamı yalnızca Orta Doğu Teknik Üniversitesi kullancılarının erişimine açılsın. (Bu seçenekle tezinizin fotokopisi ya da elektronik kopyası Kütüphane aracılığı ile ODTÜ dışına dağıtılmayacaktır.) □

3. Tezim bir (1) yıl süreyle erişime kapalı olsun. (Bu seçenekle tezinizin fotokopisi ya da elektronik kopyası Kütüphane aracılığı ile ODTÜ dışına dağıtılmayacaktır.) ☒

Yazarın imzası Tarih