
BY

MARY N. GAICHIRI

UNITED STATES INTERNATIONAL UNIVERSITY - AFRICA

SPRING, 2019

BY

MARY N. GAICHIRI

Thesis Submitted to the School of Social Humanities in Partial Fulfilment of the Requirement for the Degree of Master of Arts in International Relations.

UNITED STATES INTERNATIONAL UNIVERSITY – AFRICA

SPRING, 2019
STUDENT’S DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, institution or university other than the United States International University in Nairobi for academic credit.

Sign: __________________ Date: __________________

Mary Nyaguthii Gaichiri (ID NO: 651562)

Supervisor’s declaration

This thesis has been presented for examination with my approval as the appointed supervisor.

Sign: __________________ Date: __________________

Mr Willis Maganda
USIU- A

Sign: __________________ Date: __________________

Prof. Martin C. Njoroge
Dean, School of Humanities and Social Sciences,
USIU- A

Sign: __________________ Date: __________________

Ambassador Prof. Ruthie Rono
Deputy Vice-Chancellor, Academic Affairs,
USIU- A
COPYRIGHT

All rights reserved. No part of this project should be reproduced, stored in a retrieval system, or transmitted in any form or by any means: electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright owner. Mary N. Gaichiri©2019
ABSTRACT

The study sought to examine the role of the UN in dealing with Cyber Insecurity between 2007 and 2017. The study focused on the following specific objectives: to examine the role of the UN Charter in dealing with the threat of cyber insecurity; to analyse the role of the UN system in dealing with cyber insecurity in the international system; and to examine the challenges facing the UN in dealing with Cyber Insecurity.

The target population of this study was the international systems while the study area was the United Nations (UN). The investigation utilized exploratory research design whereby qualitative as well secondary data from the World Values Surveys, government records, non-profit organisations (NGOs) records, media articles, and studies related to the current topic was the key source of information. Secondary data was analyzed using content and principle component analysis. Qualitative data as well as secondary data was analyzed using content and principle component analysis.

Regarding the role of UN Charter in dealing with the threat of cyber insecurity the analysis has established that UN Charter can only achieve its overarching purposes of maintaining international peace and security and to save succeeding generations from the scourges of war if it prohibits the resort to any forcible measure likely to provoke military counter-force and, ultimately, the outbreak of international armed conflict. The study has also established that stability among states in cyberspace is under pressure because of the lack of agreed norms of behaviour. The findings show that not exclusively should there be an outfitted assault to legitimize the utilization military power in self-protection, however the assault must be noteworthy; it must be inferable from the state where the self-preservation is being completed; the utilization of power must be a final retreat and should probably prevail with regards to accomplishing guard, and should be proportionate to the damage endured.

On the role of the UN system in dealing with cyber insecurity, the study has shown that setting up regulating structures and building trust in the shared advantages of consenting to understandings and standards of conduct will help decrease the danger of cybersecurity occurrences entering an escalatory winding of discipline and counter-discipline.

Regarding the challenges facing the UN in dealing with Cyber Insecurity, the study has established that with the expanding multiplication of data and correspondence advances and the developing open door for ongoing borderless trade, cybersecurity is a complex transnational issue that requires worldwide collaboration for guaranteeing a sheltered the internet. The analysis show that few variables make the circumstance in the internet especially hard to control. For example, the nonattendance of a typical comprehension on the appropriate global tenets for state conduct in that area, a large number of the devices in the internet can be utilized for both authentic and pernicious purposes. What's more, states and nonstate performing artists are doing progressively advanced abuses of vulnerabilities in ICT.

The study concludes that the contention must start by reference to Article 2(4) of the UN Charter as the general principle. Article 2(4) by and large forbids the utilization of
power aside from on account of self-defence as set out in Article 51 or with Security Council approval. It is clear that action at the United Nations Systems, be that as it may, has been generally drowsy. The examination concludes that the rule of need might be relevant if the demonstration of self-protection is finished with the target to return or repulse the outfitted assault. The point of self-protection isn't to respond to the mischief done however to keep the appearance of damage conceivably coming about because of a risk.

The study recommends that the case for attribution would have to be made with clear and convincing evidence. Additionally, the UN needs to have a fair system in place to punish those who have violated cyber-security. The investigation suggests that there is need to raise international awareness about crimes against information society.
DEDICATION

This study is dedicated to my late husband Mr. Denis Munene, a Cyber Security expert. I appreciate that you always pushed me to break my limits and inspired me to research on this Topic despite insurmountable challenges. May your Soul rest in eternal peace.
ACKNOWLEDGEMENT

Regardless of anything else I give my gratefulness and humble appreciation to the Almighty God for the blessing of life, incredible prosperity, a sound identity and heavenly fortune that engaged me to think about this study.

Moreover, I wish to accord my Supervisor, Mr. Willis Maganda for equipping me with the learning and aptitudes in creating the paper. I appreciate the sound guidance, expertise and encouragement all through the study by scrutinizing and reviewing my work. I also thank, Mr. Weldon Ngeno taking time to review my work and give constructive academic criticism and commendation.

Finally, and most importantly, my late husband Mr. Denis Munene for helping me formulate this idea, pointing me to the right resources that granted me access to valuable literature and helping to review my work before your demise. God bless you all.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>STUDENT'S DECLARATION</th>
<th>ii</th>
</tr>
</thead>
<tbody>
<tr>
<td>COPYRIGHT</td>
<td>iii</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td>DEDICATION</td>
<td>vi</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td>vii</td>
</tr>
<tr>
<td>1.0 INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Background to the Study</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Statement of the Problem</td>
<td>4</td>
</tr>
<tr>
<td>1.3 Objectives of the Study</td>
<td>5</td>
</tr>
<tr>
<td>1.4 Specific Objectives</td>
<td>5</td>
</tr>
<tr>
<td>1.5 Research Questions</td>
<td>6</td>
</tr>
<tr>
<td>1.6 Justification and Significance</td>
<td>6</td>
</tr>
<tr>
<td>1.7 Scope of the Study</td>
<td>6</td>
</tr>
<tr>
<td>1.8 Definitions of Key Terms</td>
<td>7</td>
</tr>
<tr>
<td>1.9 Chapter Summary</td>
<td>7</td>
</tr>
<tr>
<td>2.0 LITERATURE REVIEW</td>
<td>9</td>
</tr>
<tr>
<td>2.1 Introduction</td>
<td>9</td>
</tr>
<tr>
<td>2.2 Role of the UN Charter in Dealing with the Threat of Cyber Insecurity</td>
<td>9</td>
</tr>
<tr>
<td>2.3 International Regimes and Cyber Insecurity</td>
<td>24</td>
</tr>
<tr>
<td>2.4 Challenges Facing the UN in Dealing with Cyber Insecurity</td>
<td>26</td>
</tr>
<tr>
<td>2.5 Theoretical Framework</td>
<td>28</td>
</tr>
<tr>
<td>2.6 Chapter Summary</td>
<td>30</td>
</tr>
<tr>
<td>3.0 RESEARCH METHODOLOGY</td>
<td>32</td>
</tr>
<tr>
<td>3.1 Introduction</td>
<td>32</td>
</tr>
<tr>
<td>3.2 Research Design</td>
<td>32</td>
</tr>
<tr>
<td>3.3 Population and Sampling</td>
<td>32</td>
</tr>
<tr>
<td>3.4 Data Analysis Methods</td>
<td>32</td>
</tr>
<tr>
<td>3.5 Ethical Standards</td>
<td>33</td>
</tr>
<tr>
<td>3.6 Chapter Summary</td>
<td>33</td>
</tr>
<tr>
<td>4.0 RESULTS AND FINDINGS</td>
<td>34</td>
</tr>
<tr>
<td>4.1 Introduction</td>
<td>34</td>
</tr>
<tr>
<td>4.2 The Role of the UN Charter in Dealing with the Threat of Cyber Insecurity</td>
<td>34</td>
</tr>
</tbody>
</table>
4.3 The Role of the UN System in Dealing with Cyber Insecurity in the International System..................................................................................................................36
4.4 Challenges Facing the UN in Dealing with Cyber Insecurity...........................................38

5.0 DISCUSSION, CONCLUSION AND RECOMMENDATIONS ..................40
5.1 Introduction...................................................................................................................40
5.2 Summary of Findings...............................................................................................40
5.3 Discussion..................................................................................................................42
5.4 Conclusions................................................................................................................46
5.5 Recommendations.....................................................................................................48

REFERENCES.................................................................................................................50
CHAPTER ONE

1.0 INTRODUCTION

1.1 Background to the Study

Article one of the UN Charter outlines the four main purposes of its formation, key amongst this being the maintenance of international peace and security. Whilst throughout history, states have waged war in order to advance national interests in an ever-changing international game of power (Trias, 2013), the dynamics of warfare and inter-state interactions keep evolving. From the sword battles of the past to the unmanned drone strikes of today, this game of power is constantly driven to shift and evolve majorly by technology. The development of armoured vehicles, aircraft, ships and the use of electronics and telecommunications have all expanded the battle space and introduced new and innovative ways to gain an advantage over opponents (Waxman, 2015). Just as the technological innovation of flight triggered a race to dominate the skies, the emergence of cyberspace has opened up new strategic possibilities and threats, causing a scramble to secure a dominant position inside of it (Swanson, 2013). It is created, maintained, owned and operated collectively by public and private stakeholders across the globe and changes constantly in response to technological innovation (Bell, 2013). Cyberspace not being subject to geopolitical or natural boundaries, information and electronic payloads are deployed instantaneously between any point of origin and any destination connected through the electromagnetic spectrum (Varin, 2015).

Increasing media coverage of cyber warfare has only served to heighten public awareness that cyberspace is becoming an arena of warfare (Manson, 2013). Governments, too, are fully aware of the need to take action in response to threats from cyberspace. For instance, documents leaked from the National Security Agency in the United States (US) confirm that national security figures are seeking to establish offensive cyber capability (McIsaak, 2013). In the United Kingdom (UK), government officials have warned of a lack of preparedness for cyber warfare and have announced new investments to bolster defence, such as the National Cyber Security Programme (Meilinger, 2013). The North Atlantic Treaty Organization (NATO) has also been raising awareness, releasing the Tallinn Manual on the International Law Applicable to
Cyber Warfare as an attempt to advise states on how to operate legally in this new war fighting domain. Looking at this evidence, it is clear that cyber insecurity is a topic of global concern (Douhet, 2014).

The UN Charter lists as an example of unarmed enforcement the “complete or partial interruption of telegraphic, radio, and other means of communication” thus providing an express basis for UN-sanctioned cyber blockades regardless of whether the relevant threat to the peace arises in cyberspace (UNSC, 2013). While there can be no doubt that this provision also applies where the relevant threat to the peace arises in cyberspace, a textual reading of Article 42 of the UN Charter seems to provide a basis for armed enforcement action only “by air, sea, or land forces” (Wakio, 2014). This may raise the question of whether forces operating in the separate domains of space and cyberspace are excluded. Clearly, the UNSC notes that the purpose of Article 42 of the UN Charter was not to restrict the means of enforcement available to the UNSC but to extend them, where need be, to all armed services available to the leading military powers of the drafting period.

Arguably, from a teleological perspective, UN Charter can only achieve its overarching purposes of maintaining international peace and security, and “to save succeeding generations from the scourges of cyber warfare, if it prohibits the resort to any forcible measure likely to provoke military counter-force and, ultimately, the outbreak of international armed conflict (Nzavi, 2012). As a matter of logic, the Charter cannot allow that the prohibition of interstate force be circumvented by the application of non-violent means and methods which, for all intents and purposes, are equivalent to a breach of the peace between the involved states. For instance, the crippling effect of cyber operations disabling the electrical power grids of major cities, the incapacitation of systems controlling industrial production, or the infiltration of malware designed to “blind” an entire air defence system (Thiankolu, 2013).

Since the mid-1990s, the worldwide internet usage is rising continuous and so more and more sensitive transactions of everyday life are done via the cyberspace (Farwell, 2015). The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes is broadly what cyberwars constitute (Jensen, 2013).
Iran has over time seen itself as a revolutionary power and this extends into cyberspace as well (Markoff, 2014). The State has been the most persistent conducting disruptive attacks meant to disrupt US companies and infrastructure, especially banks (Cetron, 2015). Fortunately, as with China, the larger improving diplomatic situation with the US has helped to throttle back the worst offenses (Yorke, 2013). Since the nuclear agreement was signed, Iranian behavior is reported to be less disruptive, instead focusing on traditional political and military intelligence (Blank, 2012). Should the deal unwind, Iran would almost certainly act out using a wide range of means, including cyber disruption (Ashmore, 2015).

The UN Member States have conferred on the UNSC the primary responsibility for the maintenance of international peace and security (Chun, 2013). To the extent that cyber operations can adversely affect the international relations between states, there can be no doubt that the Council’s responsibility also extends to maintaining international peace and security in cyberspace. When the UNSC determines the existence of a “breach of the peace”, an “act of aggression” or, most commonly, a “threat to the peace”, it can undertake or authorize such measures as may be necessary to maintain or restore international peace and security (Saad, 2013). Such measures may be limited to issuing recommendations or calling on the involved parties to comply with provisional measures but may also involve armed and unarmed enforcement (Klimburg, 2014; & Bazan, 2015).

According to the International Court of Justice (ICJ), the prohibition applies “to any use of force, regardless of the weapons employed (Bowett, 2013). Indeed, it is relatively uncontroversial that cyber operations fall under the prohibition of Article 2(4) of the UN Charter once their effects are comparable to those likely to result from kinetic, chemical, biological or nuclear weaponry (UN Charter, 2012). This would certainly include the use of cyber operations as an offensive or defensive tool designed to cause death or injury to persons or the destruction of objects and infrastructure, irrespective of whether such destruction involves physical damage, functional harm, or a combination of both (Kaiser, 2012).

Conspicuous examples of a use of “force” within the meaning of Article 2(4) of the UN Charter, therefore, would be cyber operations manipulating target computers systems so as to cause a meltdown in a nuclear power station, or opening the floodgates of a
dam above a densely populated area, or disabling a busy airport’s air traffic control during bad weather conditions, each with potentially horrendous consequences in terms of death, injury and destruction (Schmitt, 2014). The real difficulty arises, however, with regard to the qualification as a use of “force” of cyber operations that do not, or not directly, cause death, injury or destruction. The travaux préparatoires of the UN Charter clearly show that the prohibition of “force” was not intended to extend to economic coercion and political pressures (Michael, 2013).

1.2 Statement of the Problem

Cyber-crime is an international problem which does not respect national borders. Many states have initiated policy measures to achieve the security of the ICT infrastructure. However, without international cooperation, these national measures are inadequate against transnational cybercrime and its evolved variant cyber terrorism. The specific problem is that there has not been concerted efforts by the international community to combat cybercrime (Weisskopf, 2014). The UN needs support from member states and the international community, but that has been lacking (Steiner, 2013). A key challenge of cyberspace is that it is populated by both state and non-state actors. It is for the sovereign states to ensure that non-state actors within their jurisdiction respect the law, including international legal obligations that have been incorporated into national law. Combating cybercrime and terror would not be an impossible mission when all states share this common perception (Scott, 2015). In addition to the absence of a common understanding on the applicable international rules for state behaviour in that domain, many of the tools in cyberspace can be used for both legitimate and malicious purposes (Rommes, 2014).

States and non-state actors are carrying out increasingly sophisticated exploitations of vulnerabilities in cyber space. Attribution to a specific perpetrator continues to be difficult, increasing the risk of “false flag” attacks, that is, attacks by a state, group, or individual under an assumed identity. Over the last two years, the accelerating cost of cybercrime is at 23 percent in 2017 more than 2016 and is costing organizations, on average, US$11.7 million. Whether managing incidents themselves or spending to recover from the disruption to the business and customers, organizations are investing on an unprecedented scale, but current spending priorities show that much of this is misdirected toward security capabilities that fail to deliver the greatest efficiency and
effectiveness. It is against this background the present study is motivated to examine the effectiveness of the UN in combating Cyber Insecurity.

Lockheed Martin Corp (LMT.N), which is the main provider of various information technology solutions to the United States government states that the number of worldwide cyber-attacks have quadrupled since the Estonian attacks of 2007. Number of cyber-attacks has risen sharply from 27% in 2015 to 36 percent in 2017. According to Cornish (2015), there were 500,000 malicious applications in 2015 and in 2016 that number increased to 2.5 million (Hansen, 2016). In 2018, it sits at 3.5 million (Guetzkow, 2018). The cost of damages from cybercrime is predicted to hit $6 trillion annually by 2021 compared to $3 billion in 2016 whereby global Ransomware costs are expected to have grown beyond $5 billion in 2017. An increase from $325 million in 2007, a 15-fold rise in ten years (Setser, 2013) According to Setser, the potential cost of cybercrime across the globe is $500 billion, and a data breach will cost the average company about $3.8 million. A 2017 report by a Danish shipping company: AP Moller-Maersk stated that cyber insecurity had dented profitability by $250-300 million, on account of reduced volumes and increasing unit costs. The damage at around $140 million also hit British multinational Reckitt Benckiser, maker of household-name pharmaceuticals and cleaning products.

1.3 Objectives of the Study

The purpose of this study was to examine the role of the United Nations in dealing with cyber insecurity for the period between 2007 and 2017.

1.4 Specific Objectives

The following specific objectives guided the study:

1. To examine the role of the UN Charter in dealing with the threat of cyber insecurity.

2. To analyse the role of the UN system in dealing with cyber insecurity in the international system.

3. To examine the challenges facing the UN in dealing with Cyber Insecurity.
1.5 Research Questions

1. What is the role of the UN in dealing with the threat of cyber insecurity?

2. What is the role of the UN system in dealing with cyber insecurity in the international system?

3. What are the challenges facing the UN in dealing with Cyber Insecurity?

1.6 Justification and Significance

Cyber-crime is an international problem which does not respect national borders. Most of the nations have initiated policy measures to achieve the security of the ICT infrastructure. However, without international cooperation, these national measures are inadequate against transnational cybercrime and its evolved variant cyber terrorism.

The findings of the study may help the UN Security Council to come up with a multi-stakeholder model, where state-based actors work with corporations and individuals to develop functional models of international governance.

In future, other researchers and scholars will seek to extend further studies on the role of UN in combating cyber insecurity. This study is therefore important to future researchers as it could be used as a source for future references and citation to improve the body of knowledge in this field of cyber insecurity.

The results of this study may also benefit nations involved in cyber warfare to practice norms of action in cyber security and develop shared norms of behaviour.

1.7 Scope of the Study

Literature gap, theory and policy gap.

This study examined the role of the UN in dealing with Cyber Insecurity. Secondary data for a period of 10 years (2007-2017) was used to answer the research questions: what is the role of the UN Charter in dealing with the threat of cyber insecurity?; what is the role of the UN system in dealing with cyber insecurity in the international system?; and what are the challenges facing the UN in dealing with Cyber Insecurity?
World Values Surveys, UN records, Government Records, and non-benefit associations (NGOs) records were the main sources of secondary data for the study.

1.8 Definitions of Key Terms

1.8.1 UN Charter

Also known as the Charter of the United Nations of 1945 is the foundational treaty of the United Nations, an intergovernmental organization (Senga, 2015).

1.8.2 UN System

Consists of the United Nations, and the six principal organs of the United Nations: The General Assembly, Security Council, Economic and Social Council (ECOSOC), Trusteeship Council, International Court of Justice (ICJ), and the UN Secretariat, specialized agencies, and affiliated organizations (Bruce, 2013).

1.8.3 Cyber Insecurity

Identifies the risks and threats to the system upon which we become more dependent every day and the means to overcome them (Zachary, 2015).

1.8.4 Cyber Space

Refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication (Mbakari, 2014).

1.8.5 Force In Article 2(4) of the UN Charter force is practically synonymous to “armed” or “military” force (Setser, 2013).

1.9 Chapter Summary

Chapter one has discussed the introduction of the study focusing on the problem statement, objectives of the study, justification of the study, and scope of the study. Chapter two focused on literature that focus scholars who have analysed the effectiveness of the UN system in combating cyber insecurity in the international system and the challenges facing the UN in combating Cyber Insecurity. The literature review and analysis were done through a realism and securitization theory lens. Chapter
three of the study outlined the methodology to undertake the study. The study used secondary data as the main data for analysis. Chapter three also discussed other techniques applied to undertake this study. Chapter four provided the study findings and analysis in line with the study objectives. Chapter five offered the conclusion outlining the gaps in international law that could create effective mechanisms that foster inter-state cooperation in the Cyber space. Finally, the chapter provided recommendations of the study in line with the study findings.
CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

The chapter analyses the effectiveness of United Nations Security Council on Cyberwar in view of the particular research targets. The chapter displays theoretical writing in perspective of the independent variables (UN Charter; Deterrence; & Sanctions) lastly synopsis of the literature review.

2.2 Role of the UN Charter in Dealing with the Threat of Cyber Insecurity

2.2.1 The UN Charter on the use of Force

A study done by Morgus (2012) on cyber warfare between USA, China and Russia contends that The UN Charter represents one of the primary sources of international law concerning the security of the international community, which urges states to refrain from the ‘use of force. The study found that the main aim of the state is to maintain its cyberspace free from espionage and other malicious activities. The analysis notes that USA, China, Russia are some of those countries whose cyberspace is well protected than any other countries round the globe. The study argues that, in these states the reliance of military units is very high which gives the possibility of invention of fifth dimension for war.

Vieth (2015) conducted an empirical analysis on the impact of UN charter on cybercrimes in North Korea. The study found a positive effect on the international community’s support for strict compliance with the UN Charter rules on use of force. According to the analysis, together with the UN Charter, the International Court of Justice (ICJ) in six cases has pointed to important rules of customary international law and general principles relevant to the lawful resort to the use of force. The study argues that not only must there be an armed attack to justify the use military force in self-defence, but the attack must be significant; it must be attributable to the state where the self-defence is being carried out; the use of force must be a last resort and must be likely to succeed in achieving defence, and must be proportionate to the injury suffered.
Ratnesar (2013) did a detailed analysis on the roles of UN Charter in fighting cybercrimes in Europe and Russia and noted that sponsored cyber operations qualifying as a use of “force” against another state would not only fall under the general prohibition of Article 2(4) of the UN Charter, but would normally also trigger an international armed conflict. The analysis argues that cyber operations below the threshold of “force”, even if otherwise prohibited under the customary principle of non-intervention, on the other hand, may represent lawful counter-measures in response to internationally wrongful acts not reaching the threshold of “armed attack” by another state. In addition, the analysis notes that the occurrence of cyber operations amounting to an “armed attack” permits the attacked state to exercise its inherent right to self-defence through means otherwise prohibited by the Charter including, most notably, the resort to force.

Rommesh (2014) conducted a cross sectional analysis on the extent of cybercrimes in America and China. The analysis noted that the practical relevance of the determination that cyber operations amount to a “threat to the peace”, “breach of the peace” or “act of aggression” is that it allows the UN Security Council to take forcible measures, including military force in order to maintain or restore international peace and security irrespective of the qualification of the cyber operations in question as “force” or “armed attack” under Articles 2(4) and 51 of the UN Charter. The analysis noted that all members of the United Nations as per the UN charter shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations. The analysis argues that in the absence of a treaty definition, the concept of “force” must be interpreted in good faith in accordance with the ordinary meaning to be given to the term in its context and in the light of the Charter’s object and purpose.

Comolli (2013) did an empirical review on prevalence of cyber-attacks in Russia and America and the findings shows that the Stuxnet attack while unlawful was not the equivalent of an armed attack. Secondly, attribution has not been affirmed at the international evidentiary standard in any of the three cases. State practice indicates that the case for attribution would have to be made with clear and convincing evidence. Existing literature has argued in the case of cyber-attacks generally, convincing
evidence is hard to find: Given the anonymity of the technology involved, attribution of a cyber-attack to a specific state may be very difficult. The analysis shows that while a victim state might ultimately succeed in tracing a cyber-attack to a specific server in another state, this can be an exceptionally time-consuming process, and even then, it may be impossible to definitively identify the entity or individual directing the attack.

A study done by Randazzo (2014) contends that although the ordinary meaning of “force” is clearly broad enough to include both armed and unarmed forms of coercion. This does not necessarily mean that the prohibition of interstate force is limited to the application of kinetic, chemical, biological or nuclear weaponry. According to the study, the prohibition applies to any use of force regardless of the weapons employed. Indeed, the study argues that it is relatively uncontroversial that cyber operations fall under the prohibition of Article 2(4) of the UN Charter once their effects are comparable to those likely to result from kinetic, chemical, biological or nuclear weaponry. George, (2013) posits that this would certainly include the use of cyber operations as an offensive or defensive tool designed to cause death or injury to persons or the destruction of objects and infrastructure, irrespective of whether such destruction involves physical damage, functional harm, or a combination of both. Randazzo (2014) argues that the real difficulty arises, however, regarding the qualification as a use of “force” of cyber operations that do not, or not directly, cause death, injury or destruction. George, (2013) contends that the travaux preparatoires of the UN Charter clearly show that the prohibition of “force” was not intended to extend to economic coercion and political pressures.

Mulvenon (2013) quotes Article 41 of the UN Charter which refers to interruption of communication as a measure not involving armed force, thus suggesting that certain denial of service attacks (DOS) would not fall under the prohibition of Article 2(4). However, this does not warrant the conclusion that, absent violent effects, all cyber operations necessarily fall short of armed force. While Wilberforce (2013) has early on proposed a complex list of indicative criteria for the distinction between armed force and economic or political coercion in the cyber domain, Mulvenon (2013) pointed out qualitative, quantitative and temporal weaknesses in these criteria which illustrate, rather than remove, the continued lack of clarity in this respect.
Arguably, from a teleological perspective, Forrest (2013) posits that the Charter can only achieve its overarching purposes of maintaining international peace and security and to save succeeding generations from the scourges of war if it prohibits the resort to any forcible measure likely to provoke military counter-force and, ultimately, the outbreak of international armed conflict. As a matter of logic, Forrest (2013) argues that the Charter cannot allow that the prohibition of interstate force be circumvented by the application of non-violent means and methods which, for all intents and purposes, are equivalent to a breach of the peace between the involved states. For instance, Miller (2013) the crippling effect of cyber operations disabling the electrical power grids of major cities, the incapacitation of systems controlling industrial production, or the infiltration of malware designed to “blind” an entire air defence system. In this context, it should also be noted that Article 2(4) of the UN Charter prohibits the resort to force between states regardless of magnitude or duration.

Merkel (2014) posits that as the International Court of Justice (ICJ) clarified in its Nicaragua Case, even minor acts of interstate force fall under the general prohibition of Article 2(4) of the UN Charter, regardless of whether they also qualify as acts of “aggression”, or as “armed attacks” entitling the targeted state to resort to force in self-defence. This interpretation is reinforced by the approach taken in International humanitarian law, according to which even minor instances of armed force occurring between states are sufficient to trigger an international armed conflict. Walter (2016) argues that it would hardly make sense for Article 2(4) of the UN Charter, as the primary norm aiming to safeguard international peace and security, not to systematically prohibit all forms of interstate conduct sufficient to give rise to an international armed conflict within the meaning of Article 2 common to the Geneva Conventions. In fact, the UN Charter even goes further and prohibits not only the actual use, but already the threat of force in interstate relations.

2.2.2 Effect of International Law on Cyber Insecurity

Nakashima (2015) notes that as recognized by the International Court of Justice (ICJ), neutrality is a fundamental principle of international law that applies whatever type of weapons might be used. In a situation of international armed conflict, a neutral state is obliged to prevent its territory from being used by the belligerents, a notion which can be interpreted to include cyberspace. According to Nakashima (2015), the belligerents
in turn must respect the inviolability of neutral territory and are forbidden to move
troops, or convoys of either munitions of war or supplies across the territory of a neutral
Power. The Convention further provides that neutral states are not called upon to forbid
or restrict the use on behalf of the belligerents of telegraph or telephone cables or of
wireless telegraphy apparatus belonging to it or to companies or private individuals as
long as it applies the same policy towards all belligerents. In addition, Yegulalp (2014)
posits that this provision is of relevance for the context of cyber warfare because the
target or destination of cyber operations can generally be determined with precision
although their geographical routing cannot normally be controlled so as to completely
avoid the use of neutral telecommunications infrastructure.

The question according to Wright (2015) is therefore, whether the information and
payloads transmitted by the belligerents through neutral cyber infrastructure constitute
actual weapons systems which would violate the law of neutrality or mere
communication data which would be permissible. From a technical point of view,
Lawrence (2014) argues that depending on the precise nature and design of the cyber
operation in question, either option can be the case. For instance, Botnets (2013) posits
that the large quantities of communication data used to flood selected servers in denial
of service attacks could hardly, as such, be regarded as a weapons system, whereas the
contrary may have to be concluded in case of payloads being reconstituted at their
destination with elements of local infrastructure and data to provide a destructive attack
capability.

An empirical analysis done by Clay (2013) notes that the rationale of exempting neutral
powers from controlling the use on behalf of the belligerents of telegraph or telephone
cables or of wireless telegraphy was not, however, to distinguish between
communications and weapons systems as much as it simply reflected the impossibility
of the task of controlling the extraterritorially initiated use of publicly accessible
transnational communications networks. The analysis contends that where the neutral
state exercises territorial control, on the other hand, the Convention expressly prohibits
that belligerents “(a) Erect on the territory of a neutral Power a wireless telegraphy
station or other apparatus for the purpose of communicating with belligerent forces on
land or sea; (b) Use any installation of this kind established by them before the war on
the territory of a neutral power for purely military purposes and which has not been opened for the service of public messages.

Mark (2015) conducted a detailed literature analysis on the effect of international law on cyber war and noted that the exact same rationale underlying The Hague Convention would suggest that neutral states can be expected to prevent belligerent states from conducting cyber hostilities from within their territory, but not the routing of belligerent cyber operations through their publicly accessible communications infrastructure. Similarly, Gregory (2015) contends that the law of neutrality applies only in international armed conflict. However, Mark (2015) asserts that the pragmatic logic of its core principles has already found its way into the practice of non-international armed conflicts as well. The practical consequences of non-state belligerents abusing “neutral” territory to conduct attacks against other states are not unlike those foreseen in the traditional law of neutrality and include most notably, the loss of the neutral territory’s inviolability.

Verton (2014) found that as has been seen in connection with the attacks conducted by Al-Qaida against the US from within Afghanistan, by Hezbollah against Israel from within Lebanon, and by the Fuerzas Armadas Revolucionarias de Colombia (FARC) against Colombia from within Ecuador, the attacked states have conducted extraterritorial military interventions directly against the respective groups because their “neutral” host states were either unable or unwilling to protect the attacked states’ interests within their territory. While the permissibility of such extraterritorial incursions remains widely controversial in view of the UN Charter regime regulating the use of interstate force, Verton (2014) argues that the basic obligation of states to prevent hostile activities against other states from within their territory appears to be widely recognized, although normally expressed in terms of the principle of non-intervention rather than that of neutrality.

Tang (2013) in a study done to establish the effect of UN Charter on fight against cybercrime notes that the International Humanitarian Law (IHL), described as the “law of armed conflict” or jus in bello, applies exclusively in situations of armed conflict and regulates the conduct of hostilities between the belligerent parties, as well as the protection and treatment of those having fallen into the power of the enemy. The most important sources of IHL are the four Geneva Conventions of 1949 (GC I–IV) and their
first two Additional Protocols of 1977 (AP I and II), as well as the Regulations annexed to the Fourth Hague Convention of 1907 (H IV R) and a series of treaties prohibiting or restricting the use of certain weapons. Additionally, Pierre (2013) argues that in the course of decades and centuries of warfare, a rich body of customary IHL has developed which proves helpful in cases not regulated by applicable treaty law. The question of whether cyber operations can amount to war, warfare, armed conflict or hostilities raises preliminary questions of definition and terminology. According to Pierre, for the time being, the notions of “cyberwar”, “cyber warfare”, “cyber hostilities” and “cyber conflict” have not been authoritatively defined for the purposes of international law. The only treaty definition that exists, by the regional Shanghai Cooperation Organization, concerns the wider concept of “information war”, which Swartz (2015) define as confrontation between two or more states in the information space aimed at damaging information systems, processes, resources, other structures, undermining political, economic and social systems, mass psychological brainwashing to destabilize society and state, as well as to force the state to taking decisions in the interest of an opposing party.

Shawness (2016) averred that the term “information warfare” is often inaccurately used as a synonym for “information operations” while the latter can occur both in times of peace and of war, the former refers exclusively to information operations conducted in situations of armed conflict and excludes information operations occurring during peacetime. Applied to the more specific context of cyber operations, this means that the use of the term “cyberwar”, “cyber warfare”, “cyber hostilities” and “cyber conflict” should be restricted to armed conflicts within the meaning of IHL. Indeed, security threats emanating from cyberspace which do not reach the threshold of armed conflict can be described as “cybercrime”, “cyber operations”, “cyber policing” or, where appropriate, as cyber terrorism or “cyber piracy”, but should not be referred to with terminology inviting doubt and uncertainty as to the applicability of the law of armed conflict.

Fulghum (2013) did an analysis on the impact of international law on combating cyber insecurity in China and Korean peninsula and established that it appears to be uncontested that IHL applies to cyber operations which are carried out in the context of a pre-existing international or non-international armed conflict. It seems to be generally
recognized that the fact that cyber operations did not exist at the time of the drafting and adoption of most contemporary instruments of IHL does not preclude their applicability to such operations. The analysis shows that one of the most fundamental rules of IHL has always been that the right of belligerents to choose methods or means of warfare is not unlimited thus, existing IHL clearly anticipates the application of its rules and principles to newly developed methods and means of warfare.

Similarly, Sevastopulo (2014) notes that it is not the precise nature of a means or method, but the context in which it is used, which subjects it to the rules and principles of IHL. Whether a cyber-operation must be regarded as carried out in the context of an armed conflict does not necessarily depend on the territorial connection of the operation but, rather, on whether it is carried out for reasons related to an armed conflict or according to a study done by Schiffman (2016) whether it has a “nexus” with an ongoing armed conflict. This also means that cyber operations conducted for reasons unrelated to an armed conflict (lack of nexus) may qualify as cyber criminality or cyber policing among others, but are not governed by IHL, even if carried out by a belligerent party or within a territory affected by an armed conflict.

A study done by Thomas (2015) argues that here is disagreement as to whether the notion of attack also includes cyber operations aiming to merely capture or neutralize rather than kill, injure or destroy the target. The leading argument in favour of extending the effects-based interpretation of “attack” to cyber operations aiming to “neutralize” is that the treaty definition of military objectives in Article 52(2) of AP I includes objects whose “capture and neutralization” would offer a definite military advantage and puts these two alternatives on the same level as total or partial destruction. Although the term “attack” is a key notion of IHL, an analysis of the relevance of its rules on the conduct of hostilities for cyber operations cannot be limited to an examination of this notion. In line with this interpretation, a study done by Savage (2013) argues that cyber operations aiming to disrupt or incapacitate an adversary’s computer-controlled radar or weapons systems, logistic supply or communication networks may not directly cause any physical damage, but would certainly qualify as part of the hostilities and, therefore, would have to comply with the rules and principles of IHL governing the conduct of hostilities.
2.2.3 Effect of Deterrence on Cyber Insecurity

Mearsheimer (2014), notes that deterrence as a concept is not new, and its roots can be traced back to Thucydides and the Greek Peloponnesian War. In the modern era, deterrence has been applied with varying levels of success in many fields including nuclear, space, ballistic missiles, conventional build-up of military means, and even contemporary security issues like terrorism. With the increasing incidence and magnitude of cyberattacks, there is a growing interest by both academics and policymakers in applying the concept of deterrence to cyberspace. Jervis (2013) states that deterrence is largely a rational attempt to understand what can be seen as a psychological relationship with an adversarial state. Studies have shown that the effect deterrence has on state is abstract and cannot be quantified or qualified. Thus, how states behave in a given scenario may vary according to circumstance, such as the state doing the deterring and the fundamental relationship between states.

There is much debate by academics over what constitutes deterrence both in and outside cyberspace. For instance, Geers (2013) limit the discourse of deterrence in cyberspace to the classical interpretation of deterrence through denial and the threat of punishment. However, an analysis done by Glaser (2013) extend the concept of deterrence to the development of norms and the creation of interdependence among states in cyberspace. Glaser has also extended the discourse to include deterrence by futility, which is to deter would-be attackers by minimising the effects of a cyberattack. The flaw of deterrence is that it does not offer advice on how to avoid crises, or how to decide whether the national interests at stake are enough to warrant the use of military force. Accordingly, deterrence remains in the cognitive domain, and is essentially an influence operation shaped by the interplay of credibility, capability, and communication.

2.2.3.1 Deterrence by Denial and Cyber Insecurity

A study conducted by Leyden (2014) states that deterrence by denial is a strategy whereby enemies are physically prevented from obtaining technology that can threaten the existence of the state. Comparing cyber to nuclear deterrence the study argued that successful deterrence by denial must meet three criteria: capability, credibility, and communication. Capability refers to the ability to procure materiel, capacity, and the means of conducting a successful attack on a given state. There have been documented
cases where states undertake military action against another state to physically destroy their nascent nuclear infrastructure. The cost, time needed, and lack of political will may deter some states from rebuilding a clandestine nuclear programme. Through the active denial of capabilities acquisition, the adversary is thus deterred against pursuing nuclear power. The cyber equivalent of deterrence by denial would be the wholesale destruction of both the state’s computing hardware and software in cases where any possession of computing power by a potential adversary may be a threat.

However, an empirical analysis conducted by McCain (2015) found that this scenario is highly unadvisable because the technology could be used for benign operations in peacetime such as the management of health records or the streamlining of government processes. The destruction of a state’s computer infrastructure for “deterrence” would exceed the mandate that deterrence by denial confers because of the potential harm to civilians. Robert (2013) argues that the same technology may also be used to carry out espionage activity, because cyberspace is much more expedient as compared to the traditional trawling of information from physical filing cabinets. As espionage is not prohibited in international law, states seeking to use cyber tools to conduct such activities cannot be legally denied because there is no such provision against them. For instance, the analysis found that Singapore is free to conduct espionage on other states, which is widely seen as a globally accepted norm.

Jensen (2014) contends that in order to deny a state the ability to procure materiel, capacity, and the means of conducting a successful attack, the defending state must be able to verify the presence of such dangerous materiel or prove the development of offensive capability. But because cyber tools are non-physical, defending states will have difficulty conducting verification on capability belonging to potential attacking states. For instance, a study done by Herman (2013) stated that no one could have seen the Stuxnet worm crawling towards Iran, or to even detect it, when it struck the systems controlling the nuclear centrifuges. The Iranians had no way of denying their attackers this capability. This is unlike verification of nuclear weapons which can be done physically.

A study done by Johnston (2014) on cyber-attacks between 2010-2016 in Israel argues that to facilitate verification regimes also requires one state to facilitate these verification efforts by another state. However, the non-physical and non-quantifiable
nature of cyber tools makes verification almost impossible. According to study there are two more factors that will critically hinder any effort at creating a cyber-verification regime. First, cyberattacks are primarily based on vulnerabilities found in computer codes. If the defending state does not know what its vulnerabilities are, it would not be able to verify if a cyber-tool is dangerous or not. Second, no prospective attacker would want to disclose their cyber weapons for verification because the act of disclosure would enable the defending state to find a defence and render the weapons useless.

Herzog (2015) noted that credibility is the attribute of being believed. According to Herzog, the prospective attacking state must believe that the defending state is capable of inflicting damage, and at the same time, committed through its political will to use that capability. No state can credibly claim they can deny all sources of cyberattacks. The widespread proliferation of computing devices would require a herculean effort by a state to eradicate all possible sources of cyberattacks. The ease and low cost of procuring computers, servers, and software on the dark net by persons of any age and nationality mean that potentially anyone with a computer can conduct cyberattacks. Kim (2015) contends that hackers can be armed with as little as a personal laptop, be as young as 15 years old, and be anywhere in the world.

In another study done by Gorman (2013) on the fight against cybercrime, it was found that deterrence by denial also requires that the threatened costs be communicated clearly to the prospective attacking state. This can be achieved through the communication of repercussions that states or individual actors may face should they be found in contravention to what was agreed to by international treaties, laws, or mutually agreed norms. For instance, Scarborough (2013) stated that in the case of Iran’s nuclear crisis, its obligations and potential sanctions were clearly communicated in the Nuclear Non-Proliferation Treaty that it signed. This enabled sanctions to be placed on them when they failed to comply and was only lifted when they agreed to reduce their holdings of nuclear fuel and have a verification regime set up to prevent them from reneging on their commitments. Transposing this to the cyber domain, it is beneficial to have international treaties, laws, or mutually agreed norms.
2.2.3.2 Punishment and Cyber Insecurity

Gelb (2013) states that punishment as a mode of deterrence is similarly a classic way to discourage undesirable behaviour. However, there needs to be clarification that deterrence by punishment is seen as a strategy of last resort, rather than an immediate go-to policy. States can theorise about reacting to cyber incidents through the Diplomacy, Information, Military, Economic, Financial, Intelligence and, Law Enforcement (DIMEFIL) model. There is a full spectrum of punishments that can be undertaken, including economic sanctions, diplomatic protests, and show of military force. For instance, a study done by Fainaru (2014) found that five Chinese military officers were charged in absentia with cyber espionage against American corporations for commercial advantage in 2014. Subsequently, China and the US and later the UK came to an agreement not to engage in economically driven espionage. According to study, policymakers have to decide on a response that meets both the deterrent objective and the level of proportionality to the initial attack. The decision to respond in kind to a cyberattack or to create a kinetic response using conventional weapon systems must be made carefully. However, the study argues that while a cyber-response may seem logical, it can exceed the level of proportionality and may lack the precision of conventional weapons.

Grimaldi (2014) contends that the US has demonstrated proportionality in its response to several major cyberattacks which have been attributed to state actors. In the case of the 2014 cyber espionage, although the act was committed by military officers, the hacking activity was not seen to require state-on-state economic sanctions, and criminal charges were pressed instead. The study posits that adequate thought to formulate a proportional response should be given because it is a delicate exercise that may lead to escalation if not handled properly. States must gauge the level of confidence they have in their capability to attribute a case. Asserts that forensics is not perfect and if there is a lack of concrete evidence, policymakers may be hard-pressed to initiate retaliatory action even if the cybersecurity incident was serious.

A study done by Rohozinski (2014) on the extent of Russian involvement in cyber war stated that Russia to a large degree remains driven by having lost the Cold War, trying to carve out a sphere of influence in its near abroad and working to undermine the transatlantic victors, the US, Europe, and the NATO structure that unites both Since
annexing Crimea, Russian cyber operations have gone from quiet, professional political and military espionage to far more aggressive and obvious intelligence and influence operations. Similarly, China feels preyed upon by Western powers since the unequal treaties of the mid-1800s. Because China has been unfairly kept down by the West, the study notes that anything is permitted to catch back up. For most of the past fifteen years, this meant widespread and aggressive espionage for commercial purposes. It now seems that such espionage has fallen off dramatically, at least in part because of a 2015 agreement by President Obama and President Xi.

An empirical review done by Clemente (2013) shows that North Korea is starving both in the literal sense of being poor as well as feeling starved of attention. Cyber capabilities, such as that used against Sony Motion Pictures, is a way for the North Koreans to actualize their tantrums as well as have a direct, though limited, impact in South Korea and the US. North Korea knows it cannot keep pace with American and South Korean military capabilities, so cyber sabotage offers unique benefits, as does cyberwar to raise hard currency. Even so, the behaviour often closely matches the overall diplomatic environment.

Deutch (2014) notes that states must assess the damage done by the cyberattacks. Damages done include the destruction of physical infrastructure, the cost to the economy, the destabilising of society, and the harm done to national interests. For instance, while North Korea’s cyberattack on Sony caused a loss of data and reputation, there was no physical destruction of infrastructure. Hence, no punishment was initiated at that stage. Similarly, an analysis done by Ludwig (2013) found that White House had sought to undertake covert cyber operations against Russia before, but ultimately abandoned the idea of action because these plans were not thought to be particularly effective. The analysis pointed out that retaliatory action is technically illegal under the United Nations (UN) charter and may lead to an escalation of hostilities between the US and Russia. Hence, there may be a limit to the operations the state can carry out without the risk of escalation. International law also prohibits the excessive use of force to deter future attacks. In addition, some states might respond disproportionately to send a clear signal and deter future cyberattacks. However international law compels states to react in a way that is necessary and proportionate to repel or defeat a cyberattack, and in a manner that the scale, scope, duration, and intensity of the retaliatory action
are justifiable. By acting proportionally, a state may find it easier to build coalitions to address the hostile behaviour of the offending state, as well as limiting the possible escalation of the incident.

A study conducted by Datong (2013) argues that a state needs to be careful with its response because any disproportionate reaction to a cyberattack, resulting in escalation by the attacker, could be potentially catastrophic on the nation’s economy, infrastructure, and physical size. The study proposed using redlines in cyberspace to signal the response mechanisms a state may undertake should it be the target of a cyberattack. For example, attackers conducting denial-of-service attacks may face diplomatic démarche or have their behaviour exposed through the media. This sends a warning to future attackers on the consequences that they may face should they choose to act in an aggressive and hostile manner. Governments will likely come under increasing pressure to react decisively to cyberattacks, and it is suggested that they develop a framework for response so policymakers have a point of reference.

In an analysis, Anderson (2013) noted that US officials have suggested that punishment could include wide-ranging covert cyber operations devised to distress and rattle the Russian leadership, or more traditional methods such as trade sanctions in response to the perceived election meddling. Another example of what kind of redlines will trigger a reaction can be seen in the Sony hacks. Punishment against North Korea, the alleged perpetrator, was only implemented when threats to carry out 9/11 style attacks on movie theatres were made. Anderson (2013) states that this crossed a red line which was unacceptable to the US government, as it undermined its constitutional right to freedom of expression. Not defending this right would cause reputational damage to the US from both outside and within.

Mattis (2013) contends that if states are using the threat of punishment as a means of deterrence, they first need to ensure that this threat is credible. There has been increasing rhetoric worldwide over the possession of offensive cyber weapons, with states choosing to declare that they own such weapons as a form of deterrence. States like the US, the UK, and Australia have already affirmed that they will use these weapons in retaliation if cyberattacked, reacting in the same way if a physical attack was upon them. Rhetoric in cyber action may have a level of deterrence through the perceived capability of states, but there must be actualisation of this rhetoric after
calling out a perpetrator in order to maintain the credibility of this deterrence. One example being how the US turned words into action when it was discovered Russia cyberattacked their Democratic National Convention servers. 35 Russian diplomats were expelled.

**2.2.4 Concept of Self-defence in Cyber Operations**

A study done by Lehane (2014) on the effectiveness of UN Charter on fight against cyber-attacks noted that the basic function of the concept of self-defence in context to cyber operations is that the UN Charter lies in protecting the legal order by balancing the rights of an attacking state against the one who is defending. Therefore, it permits the defending state to take measures necessary to repel an armed attack, even though this may require action otherwise prohibited under international law, most notably the use of interstate force. The study notes that the justification for this permission is found in the initial wrongfulness of the offending state’s conduct and need to avert the harm likely to result from the wrongful conduct. To govern the exercise the right of self-defence is a matter of international customary law. These modalities comprise most notably the principles of necessity and proportionality. The principle of necessity defines the margin for the lawful self-defence in terms of what is objectively necessary to avert or repel an armed attack. According to the analysis, the principle of proportionality determines to what extent the harm to be prevented justifies the harm done by the defensive act.

In general, the analysis done by Lehane (2014), suggest the principle of necessity will only be applicable if the act of self-defence is done with the objective to revert or repel the armed attack. The aim of self-defence is not to react to the harm done but to prevent the materialization of harm potentially resulting from a threat. Therefore, it will be erroneous to take the claim of ‘self-defence’ after the act has been committed. Schmitt (2015) states that as per the modality of proportionality, action taken in self-defence is legally justifiable only to the extent that the harm it is expected to cause remains in reasonable proportion to the harm it aims to prevent. So, the inference that the present analysis could infer is that, Cyberspace is not permissible in response to harm which has already been done by hostile cyber operations, but only with a view to preventing or repelling an ongoing attack, and only to the extent actually necessary for that purpose.
2.2.4 Role of the UN System in Dealing with Cyber Insecurity

2.3 International Regimes and Cyber Insecurity

A study conducted by Anton (2014) noted that the stability among states in cyberspace is under pressure because of the lack of agreed norms of behaviour. Having norms in cyberspace will offer predictability, stability, and security to the international system. Facilitating cyber norms and jurisdiction exchanges is one of the pillars of nations Cybersecurity Strategy. The study argues that in the absence of universally agreed norms, the strong do what they can, and the weak suffer what they must. Attacking states can get away with little or no accountability on what they have done in cyberspace. In addition, the only factor that may be restraining the magnitude of their activities is the risk of escalation and blowback towards their own infrastructure. This still does not mean that an “electronic Pearl Harbour” will never happen; the increasingly sophisticated cyber capabilities states now have means they can be used both offensively and defensively.

Chen (2014) posits that the development of internationally agreed norms is increasingly seen as a part of every state’s arsenal for deterrence. Establishing normative frameworks and building confidence in the mutual benefits of complying with agreements and norms of behaviour will help reduce the risk of cybersecurity incidents entering an escalatory spiral of punishment and counter-punishment. According to Chen, it is through these norms that states can be ordered to behave in an internationally accepted manner. If there is non-compliance, offenders will be rightly punished based upon the principles of proportionality and credibility, in turn discouraging the pursuit of retaliation.

In a recent empirical review done by Kanuck (2016), work to develop agreed norms for cyberspace is underway at both global and regional levels, as well as between key actors, particularly the US, China, and Russia. Different sets of behavioural norms have been created by different international groups such as the United Nations Group of Governmental Experts (UN GGE) and the Shanghai Cooperation Organisation. Some of the proposed norms overlap, while others only address the interest of one group. The analysis shows that there have been confidence building measures from both regional organisations and private enterprises such as the Association of Southeast Asian Nations Regional Forum, Organization for Security and Co-operation in Europe
(OSCE), and Microsoft. There are also efforts made by think tanks such as the NATO Cooperative Cyber Defence Centre of Excellence and the Red Cross to draft international laws compatible with cyberspace.

In another study done by Xianbaiv (2014), So far, four seminal events regarding the creation of norms and limitations have happened between 2015 and 2016. The first was the UN Group of Governmental Experts (UN GGE) report published in July 2015, in which states reaffirmed that international law applied in cyberspace but did not elaborate how it applied. There were also a series of other norms agreed at the UN GGE, like not attacking the computer emergency response team capabilities of another state. The second of these events was the norm of not conducting economic espionage that China and U.S agreed upon in September 2015. This was later adopted in a joint statement by the G20 in November 2015, and what started off as a bilateral process has become a broadly accepted conduct.

Collin (2016) states that the fourth event was the confidence-building measures report published by the OSCE in March 2016. These events reflect the collective aspirational desires of the international community to build stability in cyberspace. Collin noted that a norms-based approach to cyber deterrence might engender deterrent effects at the state level but is unlikely to work in the case of “rogue” states or on certain non-state actors. For instance, the norm of not attacking critical information infrastructure in peacetime would not be observed by non-state actors like the Islamic State and cybercriminals. This norm was recommended by the UN GGE in 2015 and is part of a set of norms that were proposed to limit the behaviour of states. They are however non-binding in nature. Therefore, some may choose not to heed these norms, especially states that were not consulted in the GGE process.

According to a study done by Alami (2014), cyber warfare has become a key component in China’s military modernization. The country has used online incursions in its effort to become a global economic superpower, major regional military force, and key geopolitical influencer in the Pacific. In the past five years, Chinese hackers may have been responsible for more than 600 successful hacks. These include attempts to steal corporate and military secrets, as well as to gather data and information about America’s electrical power, telecommunications, and Internet infrastructure. The U.S.
seems to be saying ‘enough is enough,’ and has been reportedly been preparing sanctions against China.

An analysis conducted by Prakash (2014) shows that the sanctions could ban businesses and even individuals from using the U.S. financial system. The analysis states that with the recent shakiness in China’s financial markets, the U.S. already had a stronger position. Sanctions would be another ‘arrow in the U.S. Government’s quiver’ to weaken the Chinese economy, making it more difficult for the country’s businesses to utilize the U.S. financial system. In the past, these same types of sanctions have been effective with North Korea and most recently in the case of the Sony Pictures hack. However, the analysis indicates that one key difference is that those sanctions were essentially against North Korea’s military organizations. Any sanctions against the Chinese would likely be on businesses and individuals, creating new trade restrictions with the U.S. It has become painfully clear that even the largest corporations are incapable of preventing state sponsored cyber-attacks on their own. For instance, corporations can’t exactly hack back against state-based incursions. But the greatest challenge is often identifying the hacker. For this reason, it could be argued that international hacking should be treated as a criminal activity, much in the way other international financial crime is now treated.

Dave (2015) analysis states that ‘pre-cyber era international law applies to cyber operations, both conducted by, and directed against, states. This means that cyber events do not occur in a legal vacuum and thus states have both rights and bear obligations under international law.

2.4 Challenges Facing the UN in Dealing with Cyber Insecurity

According to a study by Zenko (2016), with the increasing proliferation of information and communication technologies (ICTs) and the growing opportunity for real-time borderless exchange, cybersecurity is a complex transnational issue that requires global cooperation for ensuring a safe cyberspace. Threats to cyberspace have increased dramatically in the past year afflicting 431 million adult victims globally or 14 adults’ victims every second, one million cybercrime victims every day. According to the study, Cybercrime has now become a business which exceeds a trillion dollars a year in online fraud, identity theft, and lost intellectual property, affecting millions of people
around the world, as well as countless businesses and the Governments of every nation. The study indicates that several factors make the situation in cyberspace particularly difficult to control. For instance, the absence of a common understanding on the applicable international rules for state behavior in that domain, many of the tools in cyberspace can be used for both legitimate and malicious purposes. In addition, states and nonstate actors are carrying out increasingly sophisticated exploitations of vulnerabilities in ICT. Attribution to a specific perpetrator continues to be difficult, increasing the risk of “false flag” attacks, that is, attacks by a state, group, or individual under an assumed identity.

Waxmann (2016) contends that Global connectivity, vulnerable technologies, and anonymity facilitate the spread of disruptive cyber activities that may cause considerable collateral damage, for instance, by spreading malware into computer networks or digital control systems that were not the primary target of the original attack. Waxmann indicates that in the post-world war II era, cyber security has evolved from a technical discipline to the strategic concept. The power of the internet, and the growing dependence upon it and the disruptive capability of cyber attackers now threaten national and international security. The nature of a security threat has changed a lot, but the internet provides a new delivery mechanism that can increase the speed, scale, and power of an attack. National critical infrastructures are now at risk. As a consequence, all future political and military conflicts will have a cyber-dimension, whose size and impact is difficult to predict. Waxmann argues that the UN Security Council must address the threat of strategic cyber-attacks with strategic responses in favor of cyber defense.

According to analysis by Kramer (2013), the nations will now have to adopt the technologies like that of deterrence, arms control and technology. However, the analysis indicates that Cyber-attacks deterrence lacks credibility because hacker skills are easy to acquire and because attackers are often able to conduct high-asymmetry attacks even while remaining anonymous to their victims. Another challenge as per the analysis is that Cyber arms controls appear unlikely because cyberspace is too big to inspect, and malicious code is even hard to define. However political will, perhaps in the wake of a future cyber-attack, could change the status-quo. The dynamic nature of Cyberspace makes it difficult to predict the next future cyber-attack, or how serious it...
could be. A key challenge for the UN Security Council is that the hacker tools and techniques required for cyber espionage are often the same as for cyber-attacks. Kramer posits that hackers today have enormous advantages over cyber defenders, including anonymity and asymmetry. In fact, if there is future war between major world powers, a significant degree of fighting will take place on the cyberspace only, and the first victim may be the internet itself. To shift the balance, the UN Systems will need to increase the trust on hardware and software. More improved defense strategies should be there. Government will also have to play active role in this action packed future.

2.5 Theoretical Framework

2.5.1 Realism

In the discipline of International Relations (IR), realists emphasises the competitive and conflictual side of international relations (Carr, 2013). Central to the realist tradition is the concept of “security.” Realism sees the insecurity of states as the main problem in international relations. It depicts the international system as a realm where “self-help” is the primary motivation; states must provide security for themselves because no other agency or actor can be counted on to do so. However, Kenneth (2012) argues that realists offer different explanations for why security is scarce, emphasizing a range of underlying mechanisms and causal factors such as man’s innate desire for power; conflicts of interest that arise between states possessing different resource endowments, economic systems, and political orders; and the “ordering principle” of international anarchy.

Carr (2013) posits that realists also propose numerous factors that can intensify or ameliorate the basic security problem, such as polarity, shifts in the overall balance of power, the “offense–defence balance,” and domestic politics. Several alternative approaches to international relations have challenged the basic realist account of the security problem, three of which are democratic peace theory, economic liberalism, and social constructivism. Furthermore, Mieshima (2013) argues that realism outlines various strategies that states can pursue in order to make themselves more secure, such as deterrence, maximizing power, international alliances, arms racing, socialization and innovation, and institutions and diplomacy. The first assumption of realism is that the nation-state (usually abbreviated to ‘state’) is the principle actor in international
relations. Other bodies exist, such as individuals and organisations, but their power is limited. Second, the state is a unitary actor. National interests, especially in times of war, lead the state to speak and act with one voice. Third, decision-makers are rational actors in the sense that rational decision-making leads to the pursuit of the national interest. Waltz (2013) states that taking actions that would make a state weak or vulnerable would not be rational. Realism suggests that all leaders, no matter what their political persuasion, recognise this as they attempt to manage their state’s affairs in order to survive in a competitive environment.

Finally, Carr (2013) indicates that states live in a context of anarchy – that is, in the absence of anyone being in charge internationally. The often-used analogy of there being ‘no one to call’ in an international emergency helps to underline this point. According to realism, within the states they typically have police forces, militaries, courts and so on. In an emergency, there is an expectation that these institutions will ‘do something’ in response. According to Carr, one weakness of realism is that it has typically relied on a gloomy view of humans derived from assuming a supposedly unchanging conflict-prone ‘human nature.’ This also leads to another weakness which is a tendency to treat politics both within and between states as involving unending competition for advantage.

### 2.5.2 Securitization Theory

Conceptualized as an attempt to offer a framework to analyse how certain issues become a security problem, securitization was developed by the Copenhagen School (CS) (Buzan, Waver & Wilde, 1998). Currently, it is still best developed in Security: A New Framework for Analysis which lays out a detailed and systematic overview of the main tenants of securitization (Kydd, 2012). Defined as a successful speech-act through which an inter-subjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat, securitization holds that security isn’t an objective (or subjective) condition (Williams, 2013), but rather that security has particular discursive and political force of doing something: securitizing, or the presentation of an issue in security terms (Jervis, 2013). In other words, as an existential threat (Levy, 2014).
According to Buzan, Waver and Wilde (1998), this framing of an issue in security terms is effected through the so-called securitizing move, the process through which a valued referent object is moved into the domain of security by discursively constructing its existence as being threatened, thus in need of urgent protection. This securitizing move depends, according to Buzan, Waver and Wilde, on a number of facilitating conditions in order to be successful. These facilitating conditions are (1) the demand internal to the speech-act of following the grammar of security (2) the social conditions regarding the position of authority for the securitizing actor; that is, the relationship between speaker and audience and thereby the likelihood of the audience accepting these claims made in a securitizing attempt and (3) features of the alleged threats that either facilitate or impede securitization.

The specifics of a securitizing move differs between sectors of society, each of which is characterized by specific ways in which distinct sub-forms or grammars of securitization tie referent objects, threats, and securitizing actors together (Doyle 2009). These five sectors are (1) the political (2) the economic (3) the military (4) the societal and (5) the environmental; serve as analytical devices to discern the various applications and dynamics of securitization (Dickenson, 2014). So, security issues are not simply ‘out there’ but rather must be articulated as problems by securitising actors (Fearon, 2011). Calling cyberwar a ‘threat to national security’, for instance, shifts cyberwar from a low priority political concern to a high priority issue that requires action, such as securing cyberspace. Securitisation theory challenges traditional approaches to security in IR and asserts that issues are not essentially threatening in themselves; rather, it is by referring to them as ‘security’ issues that they become security problems (Gleditsch, 2013).

2.6 Chapter Summary

Cyberspace has been described as a globally interconnected network of digital information and communications infrastructures, including the Internet, telecommunications networks, computer systems and the information resident therein. Most notably, cyberspace is the only domain which is entirely man-made (Warden, 2014). Cyber espionage has been defined as the clandestine gathering of information on networks or information systems by governments or enterprises to further their diplomatic, military or economic interests. For instance, the Chinese military allegedly
stole F-35 fighter jet plans from the U.S., which according to Federal Bureau of Investigation (2013) say allowed Beijing to create the J-31 fighter jet. The jus ad bellum is that body of law which governs the resort by states to force in their international relations (Korns, 2013). The following chapter three will discuss the methodology and technics to be applied to undertake the study.
CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Introduction

This chapter has various sections addressed showing the methodology applied to in undertaking this particular study with the goal of answering the key specific objectives of the study. The first section presents the research design. Next, the population and sample is discussed. Data collection techniques and analysis are presented in the next section. The analytical tool used in the analyses is also presented. Finally, the validity of the data applied and ethical issues in conducting the research are discussed as well.

3.2 Research Design

This investigation utilized exploratory research design. Exploratory research design is conducted in order to determine the nature of the problem and helps to have a better understanding of the problem (Onwuegbuzie, 2007). This was possible using secondary data and qualitative data for the period between 2013 and 2017.

3.3 Population and Sampling

3.3.1 Population

Target population of the study was the international systems while the study area was the UN. The United Nations is a global organization that brings together its member states to confront common challenges, manage shared responsibilities and exercise. With the increasing proliferation of information and communication technologies (ICTs) and the growing opportunity for real-time borderless exchange, UN is confronted with a complex transnational cyber insecurity that requires global cooperation for ensuring a safe Internet. This was the motivation in studying the effectiveness of UN in combating cyber insecurity.

3.4 Data Analysis Methods

Qualitative data in form of secondary data was analyzed using content and principle component analysis. Analysis involves observation and detailed description of objects, items or things that comprise the object of study. This approach was more appropriate
for the study because it allowed for deep, sense, detailed accounts in changing conditions.

3.5 Ethical Standards

The study depended on secondary as well as qualitative data. All information from secondary sources was properly cited and credit given to the original author. The study used pseudonyms for specific persons named in the secondary materials.

3.6 Chapter Summary

The chapter has detailed the methods used to carry out the study. The study applied exploratory design to examine the effectiveness of the UN in combating cyber insecurity. Secondary data from the World Values Surveys, government records, non-profit organisations (NGOs) records, media articles, and studies related to the current topic was the key source of information. The study eliminated all biases and limitations appropriately and accordingly by considering five key issues: - year of publication, credentials of the author, relevance of the information and research methodology. The study used content and principle component analysis to answer the research questions.

The following chapter (chapter four) presents the primary findings. The chapter also presents the analysis while interpreting the findings by comparing and contrasting with the literature reviewed.
CHAPTER FOUR

4.0 RESULTS AND FINDINGS

4.1 Introduction

This chapter discusses research findings of the study which was aimed to examine the effectiveness of the UN in combating Cyber Insecurity. The chapter presents the analysis of the findings guided by secondary data. The analyses was divided into the following sections: - first section analyzed the effectiveness of the UN Charter in dealing with the threat of cyber insecurity; the second section presented the role of the UN system in dealing with cyber insecurity in the international system while the third section did a detailed analysis on the challenges facing the UN in dealing with Cyber Insecurity.

4.2 The Role of the UN Charter in Dealing with the Threat of Cyber Insecurity

An exact investigation done by Vieth (2015) on the effect of UN sanction on cybercrimes in North Korea has set up a constructive outcome on the universal network's help for severe consistence with the UN Charter administers on utilization of power. As indicated by the investigation, together with the UN Charter, the ICJ in six cases has indicated imperative tenets of standard worldwide law and general standards significant to the legal implications to the utilization of power. The examination contends that not exclusively should there be an outfitted assault to legitimize the utilization military power in self-protection, however the assault must be noteworthy; it must be inferable from the state where the self-preservation is being completed; the utilization of power must be a final retreat and should probably prevail with regards to accomplishing guard, and should be proportionate to the damage endured.

Rommesh (2014) has noticed that the functional pertinence of the assurance that digital activities add up to a "risk to the harmony", "break of the harmony" or "demonstration of animosity" is that it permits the UN Security Council to take persuasive measures, incorporating military power so as to keep up or re-establish universal harmony and security independent of the capability of the digital tasks being referred to as "compel" or "furnished assault" under Articles 2(4) and 51 of the UN Charter. The investigation noticed that all individuals from the United Nations according to the UN sanction will
abstain in their global relations from the danger or utilization of power against the
regional respectability or political autonomy of any state, or in some other way
conflicting with the Purposes of the United Nations. The investigation contends that
without a settlement definition, the idea of "constrain" must be deciphered in
compliance with common decency as per the normal significance to be given to the
term in its specific circumstance and in the light of the Charter's article and reason.

Forrest (2013) has noticed that the Charter can just accomplish its all-encompassing
motivations behind keeping up universal harmony and security and to spare successive
ages from the scourges of war in the event that it forbids the UN to any persuasive
measure liable to incite military counter-constrain and, eventually, the episode of global
furnished clash. As an issue of rationale, Forrest (2013) contends that the Charter can't
permit that the disallowance of interstate power be dodged by the use of peaceful
methods and strategies which, in every practical sense, are proportionate to a break of
the harmony between the included states. For example Miller (2013) the devastating
impact of digital activities impairing the electrical power lattices of significant urban
areas, the crippling of frameworks controlling mechanical generation, or the penetration
of malware intended to "dazzle" a whole air guard framework.

In this unique circumstance, it ought to likewise be noticed that Article 2(4) of the UN
Charter denies the UN to constrain between states paying little respect to extent or term.
Nakashima (2015) takes note of that as perceived by the International Court of Justice
(ICJ), non-partisanship is a central standard of universal law that applies whatever kind
of weapons may be utilized. In a circumstance of global equipped clash, an impartial
state is obliged to keep its domain from being utilized by the belligerents, a thought
which can be translated to incorporate the internet.

It has been set up that that as has been found regarding the assaults led by Al-Qaida
against the US from inside Afghanistan, by Hezbollah against Israel from inside
Lebanon, and by the Fuerzas Armadas Revolucionarias de Colombia (FARC) against
Colombia from inside Ecuador, the assaulted states have led extraterritorial military
mediations legitimately against the individual gatherings in light of the fact that their
"unbiased" have states were either unfit or reluctant to ensure the assaulted states' interests inside their region. While the pass ability of such extraterritorial invasions remains broadly dubious in perspective on the UN Charter routine directing the
utilization of interstate power, Verton (2014) contends that the fundamental commitment of states to anticipate unfriendly exercises against different states from inside their region seems, by all accounts, to be generally perceived, albeit typically communicated regarding the rule of non-intercession as opposed to that of lack of bias. There is much discussion by scholastics over what establishes prevention both in and outside the internet. For example, Geers (2013) limit the talk of prevention in the internet to the established understanding of discouragement through forswearing and the risk of discipline. In any case, an examination done by Glaser (2013) stretch out the idea of discouragement to the improvement of standards and the making of relationship among states in the internet.

Glaser has additionally stretched out the talk to incorporate discouragement by purposelessness, which is to hinder would-be assailants by limiting the impacts of a cyberattack. Gelb (2013) states that discipline as a method of prevention is comparably an exemplary method to demoralize unfortunate conduct. Grimaldi (2014) fights that the US has exhibited proportionality in its reaction to a few noteworthy cyberattacks which have been ascribed to state performing artists. On account of the 2014 digital undercover work, despite the fact that the demonstration was carried out by military officers, the hacking movement was not seen to require state-on-state monetary assents, and criminal accusations were squeezed.

4.3 The Role of the UN System in Dealing with Cyber Insecurity in the International System.

Anton (2014) has noticed that the dependability among states in the internet is feeling the squeeze on account of the absence of concurred standards of conduct. Having standards in the internet will offer consistency, soundness, and security to the worldwide framework. Encouraging digital standards and purview trades is one of the mainstays of states Cybersecurity Strategy. The examination contends that without all around concurred standards, the solid do what they can, and the feeble endure what they should. Assaulting states can pull off practically no responsibility on what they have done in the internet. What's more, the main factor that might limit the size of their exercises is the danger of acceleration and blowback towards their own framework. This still does not imply that an "electronic Pearl Harbor" will never occur; the
inexorably refined digital capacities states currently have implied they can be utilized both disagreeably and protectively.

Chen (2014) has built up that the advancement of globally concurred standards is progressively observed as a piece of each state's armoury for prevention. Setting up regulating structures and building trust in the shared advantages of consenting to understandings and standards of conduct will help decrease the danger of cybersecurity occurrences entering an escalatory winding of discipline and counter-discipline. As indicated by Chen, it is through these standards that states can be requested to carry on in a universally acknowledged way. On the off chance that there is rebelliousness, guilty parties will be properly rebuffed dependent on the standards of proportionality and believability, thus debilitating the quest for striking back.

Xianbaiv (2014) has expressed that four original occasions with respect to the making of standards and confinements have occurred somewhere in the range of 2015 and 2016. The first was the UN Group of Governmental Experts (UN GGE) report distributed in July 2015, in which states reaffirmed that worldwide law connected in the internet, however did not intricate how it connected. There was additionally a progression of different standards concurred at the UN GGE, as not assaulting the PC crisis reaction group abilities of another state. The second of these occasions was the standard of not directing monetary secret activities that China and U.S settled upon in September 2015. This was later received in a joint explanation by the G20 in November 2015, and what began off as a reciprocal procedure has turned into an extensively acknowledged lead.

Prakash (2014) demonstrates that the authorizations could restrict organizations and even people from utilizing the U.S. budgetary framework. The examination expresses that with the ongoing flimsiness in China's money related markets, the U.S. as of now had a more grounded position. Authorizations would be another 'bolt in the U.S. Government's quiver' to debilitate the Chinese economy, making it progressively troublesome for the nation's organizations to use the U.S. budgetary framework. Previously, these equivalent kinds of approvals have been successful with North Korea and most as of late on account of the Sony Pictures hack. In any case, the examination demonstrates that one key contrast is that those authorizations were basically against North Korea's military associations. Any authorizations against the Chinese would probably be on organizations and people, making new exchange limitations with the
U.S. It has turned out to be horrendously certain that even the biggest partnerships are unequipped for averting state supported digital assaults without anyone else. For example, enterprises can't actually hack back against state-based invasions. In any case, the best test is regularly recognizing the programmer. Consequently, it could be contended that universal hacking ought to be treated as a crime, much in the way other global money related wrongdoing is presently treated.

4.4 Challenges Facing the UN in Dealing with Cyber Insecurity

Zenko (2016) has set up that with the expanding multiplication of data and correspondence advances (ICTs) and the developing open door for ongoing borderless trade, cybersecurity is a complex transnational issue that requires worldwide collaboration for guaranteeing a sheltered the internet. Dangers to the internet have expanded drastically in the previous year harrowing 431 million grown-up exploited people all around or 14 adults unfortunate casualties consistently, one million cybercrime exploited people each day. As per the investigation, Cybercrime has now turned into a business which surpasses a trillion dollars per year in online misrepresentation, data fraud, and lost protected innovation, influencing a great many individuals around the globe, just as innumerable organizations and the Governments of each country. The examination show that few variables make the circumstance in the internet especially hard to control. For example, the nonattendance of a typical comprehension on the appropriate global tenets for state conduct in that area, a large number of the devices in the internet can be utilized for both authentic and pernicious purposes. What's more, states and nonstate performing artists are doing progressively advanced abuses of vulnerabilities in ICT. Attribution to a particular culprit keeps on being troublesome, expanding the danger of "false banner" assaults, that is, assaults by a state, gathering, or individual under an expected personality.

Waxmann (2016) battles that Global availability, powerless advancements, and secrecy encourage the spread of problematic digital exercises that may cause extensive inadvertent blow-back, for example, by spreading malware into PC systems or computerized control frameworks that were not the essential focus of the first assault. Waxmann shows that in the post-world war II time, digital security has developed from a specialized control to the vital idea. The intensity of the web, and the developing reliance upon it and the troublesome capacity of digital aggressors currently
compromise national and global security. The idea of a security risk has changed a ton, yet the web gives another conveyance system that can build the speed, scale, and intensity of an assault. National basic foundations are presently in danger. As a result, all future political and military clashes will have a digital measurement, whose size and effect is hard to anticipate. Waxmann contends that the UN Security Council must address the risk of key digital assaults with vital reactions for digital resistance.

Kramer (2013) has set up that the states will currently need to embrace the innovations like that of discouragement, arms control and innovation. Nonetheless, the examination demonstrate that Cyber-assaults discouragement needs respectability since programmer aptitudes are anything but difficult to get and in light of the fact that aggressors are frequently ready to lead high-asymmetry assaults even while staying unknown to their unfortunate casualties. Another test according to the examination is that Cyber arms controls seem far-fetched on the grounds that the internet is too huge to review, and noxious code is even hard to characterize. Anyway, political will, maybe in the wake of a future digital assault, could change the present. The dynamic idea of Cyberspace makes it hard to foresee the following future digital assault, or how genuine it could be. A key test for the UN Security Council is that the programmer devices and systems required for digital surveillance are frequently equivalent to for digital assaults. Kramer sets that programmers today have colossal points of interest over digital protectors, including namelessness and asymmetry. Indeed, if there is future war between real world powers, a huge level of battling will occur on the internet just, and the primary unfortunate casualty might be simply the web. To move the equalization, the UN Systems should expand the trust on equipment and programming. Progressively improved barrier techniques ought to be there. Government will likewise need to assume dynamic job in this activity pressed future.
CHAPTER FIVE

5.0 SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This was the final chapter of the study. It summarized the findings of the study, drew conclusions based on the analysis of the literature reviewed, provided recommendations as well as insight in the areas for further research. The following research questions guided the chapter: what is the role of the UN Charter in dealing with the threat of cyber insecurity? what is the role of the UN system in dealing with cyber insecurity in the international system? and what are the challenges facing the UN in dealing with cyber insecurity?

5.2 Summary of Findings

The investigation of this composition revealed that The UN Charter represents to one of the essential wellsprings of worldwide law concerning the security of the universal network, which urges states to forgo the 'utilization of power. The investigation takes note of that USA, China, and Russia are a portion of those nations who’s the internet is very much secured than some other nations round the globe. The aftereffects of the investigation demonstrate that programmers in Estonia and Georgia made incredible utilization of the open doors given to them, and a basic looking digital task brought about furnished clash circumstance, that is the reason the idea of these digital tasks is presently quickly changing to digital fighting exercises.

The study found that there is presently the requirement for progressively successful and proficient the internet with the goal that the strike of future digital fighting and its effect could be limited. The experimental proof by Mueller (2015) has contended that the idea of 'furnished assault' and 'power' present in UN Charter makes extremely the ambiguous idea of these terms in setting to the International law. The investigation demonstrates that the lawful ramifications that will pursue the digital assault are extremely vital that must be comprehended when seen in connection to worldwide law. The World Summit Outcome Document of 2005 repeats the universal network's help for strict consistence with the UN Charter manages on utilization of power. Notwithstanding the UN Charter, the International Court of Justice (ICJ) in six cases has indicated essential standards of
standard global law and general standards significant to the legitimatization of the utilization of power. The findings indicated that not exclusively should there be an outfitted assault or equipped assault equal to legitimize the utilization military power in self-protection, however the assault must be critical; it must be inferable from the state where the self-preservation is being done; the utilization of power must be a final recourse and must probably prevail with regards to accomplishing safeguard, and should be proportionate to the damage endured. Be that as it may, the investigation battles that endeavoring to apply these conditions to digital power activities is troublesome, if certainly feasible.

The essential capacity of the idea of self-preservation in setting to digital tasks is that the UN Charter lies in ensuring the legitimate request by adjusting the privileges of an assaulting state against the person who is protecting. In this manner, it allows the safeguarding state to take estimates important to repulse a furnished assault, despite the fact that this may require activity generally disallowed under universal law, most prominently the utilization of interstate power. The examination takes note of that the legitimization for this consent is found in the underlying illegitimacy of the culpable state's direct and need to deflect the mischief liable to result from the unfair lead as per the examination by Lehane (2014).

All in all, some investigations analyzed in the study brought up that international law bolsters controlling the internet as a monetary and interchanges circle and contains coercive methods for reacting legitimately to digital incitements of various types. Administrative specialists from the five changeless individuals from the UN Security Council and 10 driving digital forces from all locales of the world have perceived that global law, including the standards of the law of state obligation, completely apply to state conduct in the internet. This acknowledgment speaks to a milestone venture toward general acknowledgment of the lawful structure. The 2012-2013 accord report from the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security suggested "ordinary institutional discourse with wide cooperation under the protection of the United Nations, just as standard exchange through two-sided, territorial and multilateral discussions, and other global associations."
Consequences of the investigation done by Liis (2014) demonstrate that few elements make the circumstance in the internet especially hard to control. For example, the nonattendance of a typical comprehension on the pertinent universal guidelines for state conduct in that space, a large number of the apparatuses in the internet can be utilized for both genuine and noxious purposes. Likewise, states and nonstate performing artists are doing progressively complex misuses of vulnerabilities in ICT. Attribution to a culprit keeps on being troublesome, expanding the danger of "false banner" assaults, that is, assaults by a state, gathering, or individual under an expected character.

5.3 Discussion

5.3.1 The Role of the UN Charter in Dealing with the Threat of Cyber Insecurity

The contention must start by reference to Article 2(4) of the UN Charter as the general principle. Article 2(4) by and large forbids the utilization of power aside from on account of self-defense as set out in Article 51 or with Security Council approval. Common significance of Force implies both outfitted and unarmed types of Coercion. The type of "drive" given in UN Charter is essentially equivalent words to "furnished" or "military" constrain. The genuine trouble emerges is to qualify the utilization of power in setting to cyber operations that don't, or not straightforwardly, cause demise, damage or demolition (Dunn, 2013). As an issue of rationale, the UN Charter can't permit that the denial of interstate be bypassed by the use of peaceful methods and strategies which, in every practical sense, are comparable to a rupture of the harmony between the included states.

The analysis of this study uncovered that The UN Charter addresses one of the fundamental wellsprings of overall law concerning the security of the widespread system, which urges states to renounce the 'use of intensity. The examination by Maurer (2013) observes that USA, China, Russia are a part of those states who’s the cyberspace is particularly verified than some different states round the globe. The analysis of this examination exhibit that hackers in Estonia and Georgia made mind blowing use of the open entryways given to them, and a fundamental looking advanced errand realized outfitted conflict condition that is the reason the possibility of these computerized assignments is directly rapidly changing to advanced battling works out.
The World Summit Outcome Document of 2005 rehashes the global network's help for strict consistence with the UN Charter manages on utilization of power. Notwithstanding the UN Charter, the International Court of Justice (ICJ) in six cases has indicated imperative guidelines of standard universal law and general standards applicable to the legitimatization of the utilization of power. According to the consequences of the investigation, not exclusively should there be an equipped assault or furnished assault comparable to legitimize the utilization military power in self-preservation, however the assault must be huge; it must be owing to the state where the self-protection is being done; the utilization of power must be a final retreat and should probably prevail with regards to accomplishing resistance, and must be proportionate to the damage endured.

Nonetheless, battles that endeavoring to apply these conditions to cyberspace activities is troublesome, if certainly feasible. As indicated by the examination, harm to unmistakable items happened just on account of the Stuxnet assault in Iran. This kind of harm does not meet the condition that an outfitted assault must be noteworthy to trigger Article 51. As the ICJ expressed in the Nicaragua case: 'The forbiddance of outfitted assaults may apply to the sending by a condition of furnished groups to the domain of another state, if such a task, as a result of its scale and impacts would have been delegated an equipped assault instead of a minor outskirts occurrence had it been done by a standard military. The ICJ made comparable evaluations of 'scale and impacts' of fierce activity in the Oil Platforms case, the Wall Advisory Opinion, and the DRC v Uganda case.

The essential capacity of the idea of self-defense in setting to digital tasks is that the UN Charter lies in ensuring the lawful request by adjusting the privileges of an assaulting state against the person who is shielding. In this manner, it allows the guarding state to take estimates important to repulse an equipped assault, despite the fact that this may require activity generally denied under global law, most strikingly the utilization of interstate power. The investigation takes note of that the avocation for this consent is found in the underlying imprpropriety of the culpable state's direct and need to turn away the mischief prone to result from the unfair lead. To oversee the activity the privilege of self-protection involves global standard law. These modalities include most eminently the standards of need and proportionality.
5.3.2 The Role of the UN System in Dealing with Cyber Insecurity in the International System

With the ascent in conspicuousness of issues of cybersecurity numerous measures have been received at the national and territorial dimension. The consequences of the examination show that Action at the United Nations Systems, be that as it may, has been generally drowsy. Generally, exercises since the Russia Federation at first presented a draft goal in 1998 have been hindered because of key contrasts between the Russian Federation and the US as supported by the examination by Feinstein (2014).

Be that as it may, since 2010 when the US out of the blue went about as a co-support to these goals there has been a discernable energy inside the UN frameworks on issues of cybersecurity. The digital assaults in Estonia in 2007, Georgia in 2008, and Iran in 2010, alongside the disclosures with respect to states keeping an eye on each other, have just expanded this force. In that capacity, action can be seen in different boards of trustees of the UN General Assembly including agreement being come to inside a few Groups of Governmental Experts on different issues (Robert, 2015). Be that as it may, issues of cybersecurity have likewise been seen in the UN Security Council with regards to fear-based oppressor movement, the Economic and Social Council and different backup organs and specific offices. The examination by Ferguson (2014) shows that with such a mind-boggling arrangement of bodies tending to the issues, in any case, discourse and correspondence between the different UN organs, bodies and gatherings now should be improved to empower additionally incorporated purposeful activity and standard advancement.

The UN is in charge of making the measures of conduct for states in the worldwide domain. All things considered, the span of the UN's capacity to create standards ought to stretch out to digital security. Seeing how to suitably respond to digital psychological oppression and digital assaults is in its developmental stage and should be talked about more regularly in the whole UN framework. Nonetheless, the General Assembly is the most suitable spot to begin this exchange as it is viewed as the most equitable body inside the UN, with all part states having a voice. The aftereffects of the examination suggest that The UN ought to use their preference as a standard business visionary to build up a strategy that states would actualize to anticipate and debilitate digital psychological oppressors and digital assaults.
5.3.3 The Challenges Facing the UN in Dealing with Cyber Insecurity

Only a few elements make the circumstance in the cyberspace especially hard to control. For example, the nonattendance of a typical comprehension on the relevant universal tenets for state conduct in that area, a significant number of the instruments in the cyberspace can be utilized for both authentic and pernicious purposes. Furthermore, states and nonstate performing artists are doing progressively advanced abuses of vulnerabilities in ICT. Attribution to a particular culprit keeps on being troublesome, expanding the danger of "false banner" assaults, that is, assaults by a state, gathering, or individual under an accepted character as Consequences of the investigation by Goldgeier (2013) show.

Worldwide connectivity, vulnerable advancements, and obscurity encourage the spread of troublesome digital exercises that may cause impressive inadvertent blow-back, for example, by spreading malware into PC systems or computerized control frameworks that were not the essential focus of the first assault. The specialists' gathering report features the particular dangers originating from the boundless utilization of ICTs in basic foundation, especially through supposed ICT-empowered mechanical control frameworks, for example, those utilized in atomic power plants and other basic frameworks.

The case of Estonia featured the following lessons: 1.) the need to raise global mindfulness about wrongdoings against data society 2.) Raised the topic of productivity of shared criminal help arrangements circumstance where the accepting party is reluctant to co-work. 3.) The conventional perspective on Substantive criminal law considers digital wrongdoing principal as a financially roused movement which may not be adequate to palatably react to politically persuaded digital assaults where the harmed legitimate intrigue isn't the respectability, accessibility, privacy or the best possible working and utilization of PC information, projects or systems, however the political, sacred, monetary or social structure of the state. 4.) There are frequently contrasting legitimate prerequisites for what is allowable in criminal procedures in the nations included and the aggressors may resort their exercises to wards that assaulted the nation. The consequences of the investigation show that the International law needs powerful authorization of instruments to guarantee co-task from the nation in which the assaults begin, if last declines to co-work.
The instance of Georgia highlighted the accompanying lessons: 1.) relevance of law of Armed Conflicts to digital assaults happening amid customary equipped clash. 2.) Measures accessible in national law to manage wide scale digital assaults. 3.) The privilege of the harmed state to utilize compel as a reaction against another state relies upon the dimension of contribution of the wellspring of the state. While state course as well as help of assaults can be viewed as dynamic inclusion. In this way legitimize a more grounded response, simple toleration or inaction for the source state as latent types of contribution don't make the source state as aloof types of inclusion to make source express an objective of legal military activities. 4.) Effective reaction to digital assaults of scale and type like the Georgia episode are very restricted under the law (Morgus, 2014). Vital is the advancement of successful worldwide collaboration, as there is no chance to get for a nation to arrange resistances against assaults beginning from different purviews.

5.4 Conclusions

5.4.1 The Role of the UN Charter in Dealing with the Threat of Cyber Insecurity

The essential capacity of the idea of self-preservation in setting to digital tasks is that the UN Charter lies in ensuring the lawful request by adjusting the privileges of an assaulting state against the person who is shielding. In this way, it allows the safeguarding state to take measures important to repulse an equipped assault, despite the fact that this may require activity generally precluded under worldwide law, most quiet the utilization of interstate power. When all is said and done, the examination concludes that the rule of need might be relevant if the demonstration of self-protection is finished with the target to return or repulse the outfitted assault. The point of self-protection isn't to respond to the mischief done however to keep the appearance of damage conceivably coming about because of a risk. In this way it will be mistaken to take the case of 'self-protection' after the demonstration has been submitted.

A move made in self-protection is legitimately legitimate just to the degree that the damage it is relied upon to make stays in sensible extent the mischief it expects to avert. So, the deduction that we could surmise is that, cyberspace isn't passable in light of mischief which has just been finished by unfriendly digital activities, yet just with the end goal of anticipating or repulsing a progressing assault, and just to the degree really
fundamental for that reason. It can be concluded that self-help plays a larger role in international law enforcement given the absence at the international level of both a central police force and compulsory courts.

5.4.2 The Role of the UN System in Dealing with Cyber Insecurity in the International System

It is concluded that despite the difficulties, cyberspace working gathering inside the UN framework would help manufacture mastery on the military parts of the cyberspace, add to the improvement of certainty building measures, and shape the advancement of standards for state conduct in the cyberspace. According to the investigation by Lalonde (2013), it doesn't appear to be too implausible a plan to change the UNGGE on Developments in the Field of Information and Telecommunications into a standing working gathering of the First Committee that any intrigued UN part state could join. What's more, much like the GGE, the standing working gathering would issue suggestions at regular intervals or somewhere in the vicinity.

The methods for fighting have developed during that time from the crudest innovations and strategies, to the most progressive arms stockpiles and strategies we have right now. Today, in the 21st century, innovation is progressing at an incredibly fast pace. This has brought about new types of taking up arms, a standout amongst the most risky and eminent ones being digital fighting. Since the creation of the web and its spread, new potential outcomes for "invasions" into either people, or states, have opened up. Experimental proof sets that today the world is associated like never before previously. Cell phones, PCs, "keen autos", even brilliant houses, are largely being incorporated into the world system for simpler access to data. As indicated by the current writing, it isn't just the people that are by and large increasingly associated, Governments just as mystery benefits far and wide are additionally being progressively associated by means of the virtual space, and even though the data is being verified with best dimension security and encryption, this does not anticipate subterfuge.

5.4.3 The Challenges Facing the UN in Dealing with Cyber Insecurity

With the expanding multiplication of data and correspondence advancements and the developing open door for continuous borderless trade, cybersecurity is a complex transnational issue that requires worldwide participation for guaranteeing a protected
the internet. Dangers to the cyberspace have expanded significantly in the previous year harassing 431 million grown-up exploited people all around or 14 adults unfortunate casualties consistently, one million cybercrime unfortunate casualties consistently as indicated by Zenko (2016). In this investigation, cybercrime has is indicated to have turned into a business which surpasses a trillion dollars per year in online extortion, wholesale fraud, and lost protected innovation, influencing a great many individuals around the globe, just as endless organizations and the Governments of each country.

A few variables make the circumstance in the internet especially hard to control. For example, the nonappearance of a typical comprehension on the material universal standards for state conduct in that space, a significant number of the apparatuses in the internet can be utilized for both genuine and malignant purposes as per the results of the investigation by Goldgeier (2013). Moreover, states and nonstate performers are doing progressively complex misuses of vulnerabilities in ICT. Attribution to a particular culprit keeps on being troublesome, expanding the danger of "false banner" assaults, that is, assaults by a state, gathering, or individual under an expected character.

Worldwide availability, defenseless advancements, and obscurity encourage the spread of problematic digital exercises that may cause significant inadvertent blow-back, for example, by spreading malware into PC systems or computerized control frameworks that were not the essential focus of the first assault. The specialists' gathering report features the particular dangers coming from the across the board utilization of ICTs in basic framework, especially through supposed ICT-empowered modern control frameworks, for example, those utilized in atomic power plants and other basic

5.5 Recommendations

1. That the UN charter is rendered inadequate to deal with the threat of cyber insecurity and only few generalists in international law are writing about cyberspace security. It is not surprising, therefore, that countermeasures are overlooked. Yet, countermeasures are the mechanisms through which UN Charter allows parties to carry out self-help, coercive enforcement of their rights. The analysis therefore prescribes that the case for attribution would have to be made with clear and convincing evidence as supported by McKune (2015).
2. Whilst appreciating that the UN charter by its own nature might not encompass every single international area of concern, the principles therein do acknowledge that key amongst its mandates its to prevent adversity that wars in subsequent generations. It is therefore upto the UN to aggressively cater to emerging international threats to peace that come up with advancement of technology. Therefore, the UN through the

3. In the international system and international law, there is no cohesive definition of cyber-terrorism or cyber-warfare that exists. Therefore, the analysis suggests that The UN needs to construct these definitions to create continuity in the responses within the international community. A precise definition would make it possible to identify when an attack has occurred and would define what member states should perform a set of actions. Additionally, the UN needs to have a fair system in place to punish those who have violated cyber-security. The UN systems should create the standards of behaviour for states in the international realm.

4. The results of the analysis indicate that the International law lacks effective enforcement of mechanisms to ensure co-operation from the country in which the attacks originate, if latter refuses to co-operate. The investigation suggests that there is need to raise international awareness about crimes against information society.

5. That the UN should work with member states to create a trans-national, legitimate mechanism to counter cyber insecurity. This could be through influencing international and regional norm building initiatives, treaties around improvement of information systems as well as deterrence mechanisms to avert both state and non-state actors from engaging in trans-national cybercrimes.

6. For future studies, the study recommends more mixed research method designs for impact evaluations, as qualitative data can enable a richer understanding of the effectiveness of the UN in combating Cyber Insecurity.
REFERENCES


Zenko, V. (2016). “To View or Not to View: Examining the Plain View Doctrine and Digital Evidence.” *American Journal of Criminal Jus*