ASSESSING THE IMPACT AND EFFECTS OF CYBER OPERATIONS UNDER INTERNATIONAL HUMANITARIAN LAWIN KENYA

LUKE GAFA

CS21B11/127

A DISSERTATION SUBMITTED TO THE SCHOOL LAW IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS OF UGANDA CHRISTIAN UNIVERSITY

May, 2025

UGANDA CHRISTIAN UNIVERSITY

A Centre of Excellence in the Heart of Africa

DECLARATION

I, LUKE GAFA herby declare that this research report has not been submitted for the award of a degree by this or any other University. To the best of my knowledge and belief; the research proposal contains no plagiarism except where due reference is made in the desktop research project itself.

Signature:

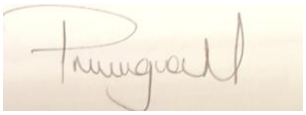
Date: 21/5/2025

LUKE GAFA

CS21B11/127

APPROVAL

This is to clarify that this research report has been written by GAFA LUKE under my supervision and is submitted for examination with my approval as the academic Supervisor.

Signature: 

Date: 20/5/2025

MS. NDURU PATRICIA

ACKNOWLEDGEMENTS

I thank the Almighty God for the wisdom and courage that enabled me to complete this research. I extend my sincere gratitude to the presence of the references given to me by Miss Nduru Patricia my supervisor. A greatly indebted supervisor who has tirelessly given effort in guidance. As a result, i was able to complete the research.

Heartfelt thanks also go to my family and friends for the support they gave me.

TABLE OF CONTENTS

Contents

ABSTRACT

Africa's development and growth of Information and Communication Technology has magnified. Digitalizing development and social economic development have coexisted, Kenya, Ethiopia and other African countries tell us the future of Armed conflict of a Non international and an International character.

Common article 3 of the Geneva conventions provides for conflict that is not of an international character between organised groups and a high contracting party, or between organised groups themselves. Organised in the sense of having a leader, with a structure of command given from him. Considering the scale and effects of cyber operations, should constitute an armed conflict in that it should be targeting the high contracting party. Prohibition of attacks against civilians also applies to cyber operations because civilians are totally protected under IHL (NIACs) unless taking participation in these cyber operations.

It is important to note that even if a cyber operation in a non international armed conflict does not rise to the level of armed conflict, that does not make the attacks legal.

CHAPTER ONE

1.0 Introduction

Cyber is an important term used to describe anything related to computers and information technology including the internet. Practically, its a broad term that covers a wide range of activities and concepts including: cyber warfare, cyber crime, cyber security and cyber culture, each of the having a definition as we shall see later on. As nations like Kenya embrace digital cyber-space systems, and are still developing their cyber capabilities and strategies, they also become targets for cybercriminals exploiting them and cyber attacks from rest of the world. The digital age brought forth a range of new and complex cyber conflicts that are reshaping the landscape of security in Africa. Data as the lifeblood of cyberspace is the main analysis of cyber, different networks, software and hardware that are interconnected to allow communication and data sharing as well as storage of data. This has become an integral part of everyone's part of modern life thus impacting everything, the way of communication especially the way of engaging armed conflict et cetera. It has changed the whole nature of armed-conflict, especially in conflict of a non international character, it has allowed the attacks that can cripple not only critical infrastructure but also civilians through disrupting communication networks often without the need for traditional force.

1.1 Background of Study

1.1.1 Cyber operations

Information dominance has had value since the world-war II as code breaking efforts not explicitly 'cyber'. The rise of computers, networks, internet and globalization intensified the use of cyber

technology for both legitimate and malicious purposes in the 1990s. The accountability of actors in cyber operations is vital majorly under International Humanitarian Law. criminal groups that have also exploited vulnerabilities for financial gain, such as ransomware attacks and data breaches, attacks on governments and individuals (NIACs). These internal armed conflicts involve government armed forces and organised armed groups, or between such groups.

The use of cyber operations continues to evolve and so does the legal framework addressing them. That International Humanitarian Law must adapt to the digital age to ensure the protection of civilians during armed conflict. In Africa, there was lack of skilled personnel in the field of information and communication technology thus a limited access to technology and a slow development to the African countries to embrace e-government initiatives. The digital economy in Africa however rapidly expanded with time driven by e-commerce, fintech, and other digital services thus adaptation. The growing awareness in Africa and all-around other states in Africa for security, gave rise to cybersecurity to protect critical infrastructure and data as seen with the African Union Convention on Cyber Security and Personal Data protection.[1]

1.1.2. International Humanitarian Law

The principles of International Humanitarian Law can be traced back to ancient civilization. There have always been limits to the brutality of war

[1] Article 7 of the African Union Convention on Cyber Security and personal data protection.

so as to protect defenceless groups. Driven by the need to codify these principles to formal laws, we see the modern movement in the 19th century.

- The Geneva Convention of 1864:

  Which focused on the protection of wounded soldiers, prisoners of war and civilians on the battlefield.

- The Hague Conventions of 1899 and 1907:

  Which addressed the means and methods to be used in warfare.

New challenges have been addressed as International Humanitarian Law keeps to evolve, such as, rise of non-state actors in armed conflict, emerging of new technologies of warfare and the evolving nature of conflict itself (NIACs). International humanitarian Law is primarily enforced through mechanism such as;

- States. States have the primary responsibility to ensure International Humanitarian Law is respected.
  - International Criminal Court (ICC). The ICC has jurisdiction to prosecute individuals for war crimes, genocide, and crimes against humanity.[2]
- International Committee of the Red Cross (ICRC). The ICRC has the unique role in promoting and monitoring compliance with International Humanitarian law as we shall see later on.[3]

[2] Article 5 of the Rome Statute
[3] Common Article 3 of the Geneva Conventions

1.2 Statement of the Problem

The focus being armed conflict not of an international character occurring in the territory of one of the high contracting parties;[4] there are standards that have to be met and must be respected by all the parties in NIACs, these include prohibitions on violence to life an persons, cruel treatment and torture. International Humanitarian Laws application is to physical warfare in terms of injury, violence, attack on objects which appears to be actual harm. Cyber crime can be looked at in two aspects; as a cyber operation whether offensive or defensive that is expected to cause injury, death to person or physical damage depending on the target and nature of the attack across various sectors of society, the other is, an operation that damages and destroys software data itself where essential services are disrupted.

Problem one is that cyberspace exists to be data which is not visible and tangible in its ordinary meaning thus creating a thin line on the threshold of harm. For example, the first scenario, *unlikely to happen*, being a building of information and communication technology (ICT) as target and attacked through attaining a virus that is capable of creating conditions that lead to overheating and potential hardware damage especially the battery that can burn or explode and burn down the building, scenario two, the buildings data being erased excluding the presence of physical damage. It is an analogy that there is damage but what kind of damage, hardware damage injury or software damage injury. There is no clear consensus on when a cyber operation crosses the threshold of an attack. One may appear as

[4] Ibid 1

an act of war the other typically less serious according to the above scenarios respectively.

Cyber warfare is constantly evolving in Kenya, with new technologies and tactics emerging rapidly. This field requires ongoing analysis to ensure that IHL remains relevant and effective in protecting civilians. Cyber operations in Kenya have been having devastating consequences for civilian and their objects, disrupting of essential services, spreading disinformation and causing widespread economic and social instability. Targeting civilian infrastructure with the potential of cyberattacks raises serious concerns about compliance of IHL principles especially proportionality and distinction including the others.

The social-economic development in Kenya has been a growth that has include both the civilian and military. Many critical infrastructure systems have both civilian and military applications such as, transportation networks, communication networks and water systems which are essential for public services and government functions. Under the computer misuse and Cybercrimes act of Kenya, critical infrastructure is defined as the processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Kenyans and the effective functions of Government.[5] Still under the same act, critical information infrastructure system or data is defined as, an information system, program or data that supports or performs a function with respect to a national critical information and infrastructure. Critical infrastructure is the foundation of contemporary society and is crucial to the development of Kenya. Critical infrastructures support not only the efficient

[5] Computer Misuse and Cybercrimes act 2018

running of companies and services but also the long-term confidence and planning in an area, and consequently continued investment levels hence blurring the lines between military targets and protected civilian objects and locations during cyberattacks.[6]

The other problem is that Kenya, like many countries in Africa, is increasingly reliant on digital infrastructure, this extends to critical sectors like finance, healthcare and government services meaning these sectors have been made vulnerable to cyber attacks, complicating and failing respect traditional notions of warfare and the application of IHL principles. The National Hospital Insurance Fund (NHIF) were allegedly hacked leading to the exposure of the personal Identifiable Information belonging to millions of Kenyans. These cyber attacks highlight the vulnerabilities of Kenya's critical infrastructure and the need for better cybersecurity measures to protect these systems from future attacks.[7]

The issue of rapid growth of cyber technology and networks appear as a challenge since there has to be reconfiguring and reengineering of security measures of these networks. It is difficult to implement effective security measures and respond to cyber threats in a timely manner, with the fact that cyber protection requires significant investment in cybersecurity tools and personnel skills.[8] These may appear as situations of internal disturbances, isolated and sporadic acts of violence however, the government of a high contracting party is being attacked by organised groups that create viruses that attack its critical infrastructure and civilian critical infrastructure.

[6] https://www.kictanet.or.ke/cyberattacks-on-critcal-infrastucture
[7] Ibid 6
[8] Ibid 7

There is possible lack of clear attribution mechanisms when placing accountability of parties in an armed conflict. That is to say it can be challenging to hold state or non state actors accountable since it appears difficult to pinpoint the source of origin of a cyber attack. With this, the states in Africa find it difficult to find who is liable for such an attack because they are still evolving to such technology thus making it difficult to find the origin of the cyber attack during an armed conflict. The national legal frame work in most countries in Africa especially Kenya, covers mainly national laws and regulations in order to address issues and provide safety and security of electronic transactions and information systems rather than addressing the complexities of cyber warfare,[9] whereas, the international legal frame work of cyberoperations in itself isn't a legal model but reflects international best practice and essential responses through customs which are not addressed legally thus no established legal framework.

The attack on data itself does not cause physical injury, or any form of physical violence. The question is whether the severity of the destruction is enough to be constituted as an armed attack? An attack on infrastructure like a power grid or devices in hospitals, can cause injury and physical damage, that is to say, they are indirect environmental consequences of an armed conflict which are violated under the core principles of International Humanitarian Law such as proportionality, humanity and distinction in that the resulting consequences can have tangible negative impacts on the environment hence creating social chaos. There are gaps in effective protection of these systems and mitigating the

[9] The Computer Misuse and Cybercrimes Act, 2018

humanitarian consequences of these attacks that is to say, complex legal and practical challenges.

1.3 Purpose and Objectives

1.3.1. General Research Objectives

This study is aimed to analyse the specific challenges of applying International Humanitarian Law principles in regulating and mitigating humanitarian consequences in cyber attacks in an armed conflict not of an international character within the Kenyan context.

1.3.2. Specific Research Objectives

i. To explore the damage caused during cyber attacks in a non international armed conflict on critical Infrastructure in Kenya.
ii. To determine whether the target and nature of attack in cyber operations respect the core principles of International Humanitarian Law.
iii. To examine the existing legal Framework within Kenya concerning cyber security and its alignment with International Humanitarian Law.

1.3.3. Research Questions

i. How do the existing international humanitarian law principles adequately address the humanitarian consequences of cyberattacks in Kenya.
ii. What role do international organisations, such as the ICRC, play in promoting IHL in the context of cyber operations in Kenya.
iii. To what extent has attribution been difficult in cyber crime under International Humanitarian Law.

1.4 Significance of the Study

The study will explore the way parties in an armed conflict have adapted to the use of cyber capabilities using them to disrupt enemy infrastructure and sowing discord among the population, since they have integrated cyber operations into their traditional military operations, using them to support conventional attacks.

1.5 Justification of the Study

Kenya like many African nations, is at a fast rate digitalizing its economy and essential services. This has increased reliance on digital infrastructure, creating vulnerabilities to cyberattacks that can possibly have devastating consequences for civilian population and objects including the government. This study shall seek to reduce risk the means and methods of cyber operations that cause harm and damage to wounded soldiers, prisoners of war and civilians and their protected objects, without which the growth of this injustice shall be immense causing exploitation of vulnerable groups in an armed conflict using cyber operations.

1.6 Scope of the Study

1.6.1. Geographical Scope

This study shall cover and focus on Kenya

1.6.2. Time Scope

The scope of this research encompasses data and information collected over the past six years, ensuring that the analysis will reflect the most current trends

1.7. Conceptual Framework

INDEPENDENT VARIABLE	**DEPENDENT VARIABLE**
Cyber operations	**Impact and effects on International Humanitarian Law**
cyber warfare cyber crime cyber security	Here the rules and principles of International Humanitarian Law are being assessed to regulate conduct in armed conflict. Distinction Proportionality Humanity Military Necessity

1.8 Literature Review

This chapter entails how well researched 'jus in bello' is in non international law in the context of cyber armed conflict; parties in an armed conflict or war need to follow the law in war, the governing principles that apply to war, however when it comes to the digital realm everything has created a need for expansion thus more research. Cyber operations during an armed conflict are operations against a computer, a computer system or network, through a data stream, when used as means and methods of warfare in the context of an armed conflict to the adversary,

AKA digital warfare. There is a massive gap that hasn't been addressed to the modernised digital warfare, which lies whether these operations respect the humane principles of traditional warfare, therefore what role cyber plays in IHL during warfare more so in non-international armed conflict.

The countries in Africa have enacted their own cybersecurity laws due to the growing awareness to protect critical infrastructure, personal data and national security from cyber threats. Cyber Security is the act of the protecting computing systems from threats like cyber harassment, unauthorised access et cetera. Section 27 (2) (b) of the computer misuse act of Kenya provides for Cyber harassment, one of the crimes in cyber, as the use of a computer for threatening to inflict injury or physical harm to the person or property of any person and is liable to imprisonment not exceeding ten years.[10] Digital warfare refers to ideologically driven cyber attacks intended to cause disruption, expert political influence over rival organised groups and states or rival between the organised groups in the states jurisdiction. On the other hand, cyber harassment involves small groups thus lacks motivations associated with warfare thus not considered digital warfare under international armed conflict however it may be addressed by non-international law and municipal law. We recognise that ICTs are the cornerstone of Kenya's social economic development and the established cyber laws that regulate, mitigate these threats and risks of malware are in existence with further increase of these crimes.

Cyber warfare as a term, is in existence because of a cyberattacks between parties and adversaries causing harm to an organised system whether digital or physical

[10] The Computer Misuse and Cybercrimes Act, 2018

using malware. For a state to be recognised it needs a government and population. Modernised governments of today have become digital governments in that societies have also transformed into digital societies. The OECD explains the aspect of how societies are transforming from physical interactions to digitally enabled solutions.[11] States bear the significant responsibility when carrying out military operations conducted under IHL and protect civilian and their objects. The belligerent parties also have a responsibility to protect the civilians and their objects. There is a gap in addressing whether state and non-state cyber armed actors as parties in a digital armed conflict have obligations to respect the laws of targeting and enhancing the distinguished line between civilian objects and military objects.

Is the principle of military necessity an exception to the above statement, to use sophisticated cyber weapons by military to inflict injury or physical harm to the adversary? With military necessity, weapons are the instrument which are used in attacks to create acts of violence against the adversary. Violence entails injury, death, damage or destruction. The notion of violence is; civilians enjoy general protection against dangers arising from military operations, however in a digital conflict its difficult for civilians to enjoy general protection against the dangers arising from the operation. No acts or threats of violence are intended to spread terror. ICRC AP commentary Article 48, the word operation should be understood in the context of the whole section, it refers to military operations during which violence is used. Acts of violence is equivalent to physical damage. Is data really a physical object that faces physical damage if attacked? (M Bothe et al).[12]

[11] OECD 'Digital Government in Chie – Digital Identity' (OECD Publishing 2019) 7
[12] Article 48 of ICRC AP commentary

Schmitt is in the view that, parties in a digital conflict will want to attack data that doesn't offer "effective contribution to military action" or yield "military advantage". Cyber operations, the IHL notion of attack is commonly understood as operations that may reasonably be expected to cause harm and injury or even death to people and their objects[13] That the targeting in a digital warfare is difficult since Digital governments inter link with the digital society. The law of targeting comprises of complex rules regarding when objects may be lawfully targeted by parties in a conflict and when such objects are immune from such targeting.

Thus, states will not accept data as an object as well as the majority of persons. We see that it is a satisfactory fact that the data isn't visible or tangible. However, malware that causes physical damage can be interpreted to qualify as a weapon under International Humanitarian Law. Whether data is an object or not, it isn't humane by the principle of humanity to make civilian objects the objects of attack. It is prohibited to use method or means of warfare which are intended or may be expected to cause damage to the natural environment and thereby to prejudice the health or survival of the population. Mr. David Mugonyi says in a report that top affected industries in brute force attack trends in Kenya include; internet service providers (ISPs), cloud service and Government.[14] These industries play vital roles in critical infrastructure sectors like hospitals, power grids and food production.[15]

[13] M. N. Schmitt and L. Vihul (eds), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
[14] Cybersecurity Report the National KE-CIRT/CC
[15] Article 14 AP II

Computers, computer networks, and cyber infrastructure may be made the object of attack if they are *military objects*.[16] I'm in the view that parties in conflict can only attack military objects if they are to use digital ware that qualifies as a weapon and means under International Humanitarian Law whether it causes physical damage, rather than attack civilian and civilian objects. However, civilians are connected to the digital government in that they will face damage if such digital ware qualifies as a weapon. Civilians are not prohibited from directly participating in cyber operations amounting to hostilities, but forfeit their protection from attacks for such time as they so participate. The threshold of harm is if the participation adversely affects military operations of party or death, injury or destruction to protect persons/objects for example cyber intelligence gathering not just cyber attacks. Direct causation may be in the aspect where there is a causal link between the act and the harm caused like developing a software specific to an attack on enemy system.

Thus, if non state armed groups are to attack data that doesn't offer 'effective contribution to military action' and causes physical damage to essential civilian infrastructure, such as power grids, water systems, foodstuffs and hospitals which are protected under International Humanitarian Law,[17] shall qualify as a weapon under International Humanitarian Law and would likely violate the principle of distinction, as a result, the parties to the conflict become liable to the civilian damage. Data itself is not typically considered a military objective unless it *directly supports military operations*. Attacks must be directly only at military objects, if not, the state and non state armed groups can be held responsible for

[16] Article 1 AP II
[17] Ibid 15

violations committed by their digital armed forces. However, determining this attribution for a cyber warfare to a specific state or specific non-state actor can be difficult at times especially with the technological advancements of the African countries since non-state actors can also be held liable if they attack on data or use malware to cause damage to civilians and civilian infrastructure. It may take time to identify actor in reliable matter. The effect may be long-delayed and you fail to know you have been attacked. One of the most concerning trends is the rise of sophisticated cyber attacks that target critical infrastructure.

Richard Baxter is in the view that International Humanitarian Law does restrict the choice of means and methods of warfare, it does protect civilians and civilian objects, however, it does not legitimize digital warfare or militarize cyberspace. The restrictive nature of International Humanitarian Law is prohibitive law that forbids rather than authorizes certain manifestations of force.[18] His observation about the restrictive nature of IHL is particularly relevant to the aspect of cyber operations. That there are many challenges in applying International Humanitarian Law to cyber warfare from the need to adapt to the existing prohibitions. For example: applying the principle of distinction between civilians and combatants in the cyberspace, since cyber operations heavily blur the line between military and civilian infrastructure since they synced in the digital realm; Applying the principle of proportionality in a cyber operation given the potential surging effects and unintended consequences (violent consequences); and applying the humanitarian principle where cyber operations can disrupt essential services especially hospitals and cause superfluous injury or unnecessary

[18] Humanizing the Laws of war edition by detlev F. Vagts by Richard Baxter

suffering, raising concerns about their humanitarian incentive.[19] For example in 2020, South Africa faced a significant ransomware attack on its healthcare system, which led to substantial disruptions in patient services and highlighted the vulnerabilities of essential public services to cyber threats. Most International Humanitarian Law rules apply in time of armed conflict but there are some that also apply in peace time. The duty to respect and ensure respect for international Humanitarian Law, rules on the protection of the distinctive emblems, duty to disseminate International Humanitarian Law in peacetime especially times of occupation.

Common article 1 of the Geneva Conventions, the ICRCs is in view that there is an obligation to conduct legal review of new weapons which also flows from the duty to ensure respect for International Humanitarian Law, since their work emphasises to protect civilians and civilian infrastructure from effects like cyber warfare. It further states that parties must respect and ensure respect for the conventions. The ICRC agree that International Humanitarian Law does apply to cyber operations in that they have an approach for any new means and methods of warfare. That there is a duty to review the legality of new weapons, means and methods. High contracting parties still have to respect their obligation under AP1 in all circumstances. States can't retaliate in a non-international armed conflict using malware because they have the obligation to determine whether the employment of a new weapon, means or method of warfare, develops, acquires or adopts would, in some or all circumstances, be prohibited by international law. In the motion of reprisals, there is a gap when it comes to attribution, there is possible difficulty in identifying thus making attribution difficult. It is crucial for

[19] Article 14 AP II

determining accountability and who is responsible and being able to retaliate or apply legal consequence.

It is a custom for states under international law to respect the law of armed conflict and the principles that govern it. The UN General Assembly Resolution defines aggression including the use of armed forces against territorial integrity of a state. It doesn't specifically address cyberoperations in a NIACs, however it provides a framework for assessing the legality of state conduct in cyberspace. We realise that the law to govern cyber operations in a NIACs, to respect the principles of International Humanitarian Law, to respect the law of targeting, to attain attribution of states or non-state actors, remains a work in progress as the use of cyber operations keeps to evolve. So too must the legal framework for addressing them.

It shall become a custom under International Humanitarian law to ethically use cyber operations and not attack military objects and civilians including their objects since there is a sync between digital government and digital society. The customary norm shall exist to protect civilians and civilian infrastructure unless participating in hostilities, the same customary norm states have to protect based on nature or severity if state are to take on cyber warfare.

1.9 Methodology

1.9.1 Introduction

This part entails the research design, target population, data collection methods encountered while carrying out the research.

1.9.2 Research design

A research design shows how the study is conducted. For the study, I shall adopt Desktop research reason being the study focus on documentation of other authors and interviews with a number of individuals.

1.9.3 Target Population

The intended target population of this study is military and civilians of the state and refugees from African countries.

1.9.4. Data Collection strategy

In carrying out this research, we shall base on a number of techniques;

Documentary Review

This method of data collection involves critically examining already existing information in the form of documents both in hard copy and soft copy relating to the topic of study. This will help us analyse articles, reports, journals and other documents of importance to establish the relationship between cyber operations and the impact it has on International Humanitarian Law.

Observation

This information will further be expanded by observation of the events and circumstances when cyber operations have been used and applied so as to

examine the impact it has on particular circumstances under International Humanitarian Law.

1.10. Limitations of the study

While carrying out this study, the researcher will be limited in gaining access to the desired respondents because of their busy schedules. This we intend to overcome by setting appointments with the respondents and respecting the appointments.

The researcher will be limited by the availability of literature in respect to cyber operations. However, I intend to overcome this by properly scrutinizing the available literature and comparing the information attained from the interviews with the available literature to achieve credible results.

1.11 Synopsis

In the event that our proposal is approved, in furtherance of our research. Chapter two will delve into the concept of cyber operations by thoroughly defining it, displaying the aspects in which it is used, reveal its impact and effects on International Humanitarian Laws. Chapter three will depict the legal framework, if there is any, on which our research will be based in regard to cyber operations in a conflict that is not of an international character. Chapter four will show case our findings in regard to our research by showing the negative impact of cyber operations in relation to International Humanitarian Law and ways to mitigate the adverse effects of the wrongful use of cyber technology during an armed conflict. Finally, chapter five will deliberate on our conclusions and recommendations pertaining to our research.

REFERENCES

Statutes

The Geneva Conventions of 12 August 1949

ICRC AP commentary

Additional Protocol II

Books

Humanizing the Laws of war edition by detlev F. Vagts by Richard Baxter

CHAPTER 2

2.0. INTRODUCTION

This chapter presents the non legal aspect of the objectives of the study. The continent with the most copper in the world is Africa. The country with the most copper mined is Democratic Republic of Congo, not only DRC but also Zambia. Copper as a complex mineral to explore and refine, requires individuals with the expertise and skills to operate such procedures. Copper is not just a mineral but it is that that is essential when it comes to building data. It acts as a conductor in transmitting electrical signals. The existence of copper breeds the existence of data, the centre of cyber. Having cyber does not necessarily mean an individual is armed. To term it as 'cyber arms', its when it is capable of causing harm and considered a weapon under International Humanitarian Law. This harm can be; disrupting of critical infrastructure like Hospitals, theft of sensitive data, manipulation of information ex cetera. Cyber armed conflict which is not of an international character might not always involve destructive attacks on infrastructure, but attacks linked to political conflicts, information and disinformation campaigns.

These conflicts have increasingly included digital technologies including cyber capabilities which have blurred the lines between traditional warfare and cyber warfare, especially the principles of traditional warfare. Targeting critical infrastructure of citizens in Kenya has become a diurnal routine. This is due to the countries wave of technology transformation that has changed both production and consumption trends which drive the social and economic development.

Ransomware attacks targeting essential services like healthcare, utilities ex cetera, these sectors are particularly vulnerable and protected under International Humanitarian Law. Unlike traditional weapons, cyber attacks do not cause immediate physical destruction but can disrupt critical infrastructure leading to a wide spread suffering of civilians. As they perform such attacks, non state actors may operate anonymously under other entities creating a significant challenge of holding parties accountable under International Humanitarian Law.

2.1 Non legal aspect on the key study objectives and study variables

2.1.1 Cyber Operations/attacks

Cyber operations is referred to as the actions done through cyberspace to achieve a specific objective. These objectives can range from, disrupting, destroying adversary's systems and infrastructure, and also protecting as an objective. However, Schmitt is in the view that, parties in conflict will want to attack data that doesn't offer "effective contribution to military action" or yield "military advantage", Parties would want to attack the digital government or the digital society, general civilian population since its a digital realm that is intangible involving computer systems that manage the economic, social and political infrastructure, like in Kenya.

Having malware in the aspect of IHL makes an individual armed since the purpose of malware is to damage and cause harm to another. Malware in the context of IHL should be considered a weapon, this is because there is intention to cause harm and disrupt. This aligns with the intent behind traditional weapons to either inflict harm or neutralize a target. Malware being the primary tool used during cyberattacks, it shall be looked at as an act of aggression in the realm of digital warfare.

2.1.2 Cyber Crime

Showcasing evolving tactics using malware and Ransome ware has emerged ever since data creation. Developing countries are adopting to such technology as it becomes essential to people's way of living and governance. Kenya is a developing state with such technology in that different laws have been established to limit cyber crime. Cyber crime is any illegal activity committed using a computer, network or data.[20] Many offences fall under cybercrime and so do the participants. In a non international conflict organised groups go against a high-contracting parties. Most of the cyber crimes happen in the aspect of armed conflict of a non international character where organised cyber groups attack the state, or between such organised arising on the territory of a state.

2.1.3 Cyber Security

With the need of privacy and other security measures from such digital threats globally, cyber security comes to play. Technologies that protect computer systems and data itself. Developing states have to evolve and adopt to such technologies. The security itself has to adopt to the data technology. Network securities and other encompassed securities protect data from unauthorised activities in the digital world. In a non international conflict the security is mandatory, however to what extent is the jurisdiction. The municipal laws of the state are put in place protect such unauthorised activities, however in an international aspect according to IHL laws aren't yet clear ethical guidelines to respect traditional principles of armed conflict.

2.1.4. Ihl and its governing principles

[20] https:// dictionary.cambridge.org/dictionary/English/cybercrime

International Humanitarian Law, well known as the law of armed conflict, has governing humane principles that are respected by the parties in the armed conflict. Distinction mandates that every attack during an armed conflict shall create a line of distinguishing between a military and civilian, military object and a civilian object. this principle is fundamental in ensuring that attacks are directed only against military targets, thus minimizing harm to innocent persons and civilian infrastructure. Balancing the damage to civilians and their infrastructure with the military necessity acquired.

Proportionality on the other hand as another principle, further establishes that even if there has been distinction and the target has only been to a military object. It requires that the anticipated civilian harm and collateral damage is not excessive. As these attacks are being made the parties in an armed conflict are to follow precautions; carefully planning to reduce the risk of incidental harm as they use methods to achieve their military goal aka military necessity.

As they take such measures, they should have the humane mentality of treating others fairly even those that can't retaliate. IHL is principles still apply for as long as there is conflict be it Cyber conflict.

2.2 The relationship between cyber operations and the principles of traditional armed conflict.

As earlier mentioned, the relationship between the government and the society in the digital realm is strong in that there is a harmonious and mutual beneficial relationship in the digital space. Citizens trust that their data is protected when interacting with the digital government services. Transparency data government policies are crucial, this makes the citizen engagement in digital services,

infrastructure and needs the same with a high contracting party. The confidence in the state as regarding the safety of civilian data shall be low in case the state is in a digital warfare with an adversary or no international actor.

The principle of distinction is the cardinal principle in place that forms part of the fabric of IHL. In both international and non international conflicts, civilians themselves and their objects at all times during an armed conflict, be it an armed conflict that involves ICTs, should be protected at all times. The obligation to direct cyber attacks only against military objectives and against civilian objects is particularly necessary. Parties who do not take direct part in part in an armed conflict have fundamental guarantees to safety. The humane treatment shall in all circumstances be paramount without any distinction. The dual use of these internet infrastructure between the military and the civilians creates a thin line of distinction if a digital war fare is to turn out. Developing states that are trying to adopt to such ICTs are also developing ways to provide security since there is an interlink of digital usage between the state and civilians. It will however be different if such digital infrastructure makes contribution to military action, the destruction must offer a definite military advantage.[21]

2.2.1 The effect of the law of targeting in matters concerning cyber operations

The parties in the conflict still have to respect certain principles of armed conflict even if the civilian digital infrastructure qualifies to be a military objective, proportionate and precautioned attacks are to used in such attacks thus the principle of proportionality and precaution are applied, However the gap of cyber operations respecting principles of traditional warfare, the cyber operation has to constitute an

[21] ICRC, https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf

"attack" or triggers IHL so as to emphasis the principles of traditional warfare, especially acts like disrupting critical civilian infrastructure. As an attack is being made, there should be the application of who to target and who not to target. Indiscriminate attacks that are of a nature to strike military objectives and civilian objects without distinction. Cyber attacks, that qualify as 'attacks' under IHL, that are not directed to a specific military objective aimed to disrupt digital systems and create possible violence are prohibited by IHL. Developing states and their developing securities to such threats find it difficult to create the line between the military and civilians when it comes to the digital realm especial in developing countries like Kenya. Kenya as a state is responsible for cyber operations conducted by their own people or organised groups and agents.

2.2.2 The effect of the developments in the field of Information and Telecommunications in establishing attribution during cyber operations in NIACs.

Parties in such a conflict that is of non international are obliged to know how IHL applies to these developments in cyberspace. In a developing country like Kenya, they have tried to establish ways to mitigate such persistent cyber threats. The National KE-CIRT/CC have recommended actions such as using strong authentication methods, maintaining regular backup of data, implementing zero trust security architecture to secure their infrastructure and data.[22] These ways have slightly decreased the APTs and brute force attacks, however more solutions and skills of security should be created so as to catch up to developments in the field of cyberspace. As stated earlier that Kenya as a state should be responsible for its cyber operations conducted by itself as a state and organised groups, this is because in the digital realm, critical civilian infrastructure that enables the provision of

[22] Cybersecurity Report the National KE-CIRT/CC

essential services and survival of civilian population. IHL provides specific protection of civilian population, their medical services and object indispensable for their survival regardless the type of the type of harmful operation.

Cyber operations often involve sophisticated techniques to cover the origin of attacks, such as proxy servers, VPNs.[23] The technical complexity in such a matter needs skills to catch such people. Establishing attribution in such a scenario is difficult and may end up failing to be established due to lack of acquired skills by developing countries like Kenya. Unlike traditional armed conflicts, cyber operations lack clear legal frameworks for attribution, making it difficult to find who is responsible. The legal field in cyberspace is a grey area especially in matters of a NIACs.[24] Developing states adopt this developing cyberspace in their essential services and find it difficult to adopt new skill in securities for such developments.

2.3 Conclusion

It is difficult for developing states especially in Africa to adopt, develop and find skills in cyber security. These significant hurdles involve both the government and the society. Security should not be a measure that is performed when a threat has happened, but it should be a measure for a future-threats, so that these future cyber threats find us prepared rather than facing them and try as much to protect critical civilian infrastructure. Skills of security are necessary in developing states especially when there is developing cyberspace.

[23] https://www.cambridge.org/core/journals/american-journal-of-international-law/article/attribution-problem-and-cyber-armed-attacks/
[24] https://unidir.org/publication/non-escalatory-attribution-of-international-cyber-incidents-facts-international-law-and-politics/

While IHL does not legitimize cyber operations, it does impose limits to protect civilians and humanitarian operations.[25] The evolving nature of cyber threats creates challenges in interpreting and enforcing effective laws. Thus it as the threats evolve, the security also evolve together with the threats.

[25] https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

CHAPTER 3

3.0 INTRODUCTION

This chapter presents the legal aspect of the objectives of the study. The international committee of the red cross (ICRC) is primarily concerned in these matters that cyber operations are used as means and methods of warfare during armed conflict, and that the traditional principles of IHL are protected. The International Covenant on Civil and Political Rights (ICCPR) mostly applied in NIACs, primarily get concerned in matters that cyber operations must respect the right to life. Cyber operations may violate this right e.g., disrupting medical systems, destroying drinking water installations.[26] These cyber operations must comply with the human rights standards. With the need to protect civilians from cyber harm in a conflict, this is an area that needs clarification. If parties in a NIAC use cyber operations to disable themselves, they must ensure the target is military, they must assess if civilian reliance on the same network, take precautions and definitely respect human rights. Kenya has established a legal framework to regulate cyber operations, through laws like the Computer Misuse and Cybercrimes Act. This legislation provides guidelines on cybersecurity management, critical information infrastructure, and cybercrime prevention

3.1 The Legal aspect on the key study objectives and key study variables.

3.1.2 Cyber Operations/ attacks

The CMCA is established to cover various offenses, including unauthorized access, cyber espionage, phishing, cyberterrorism, and more.[27] Most of these existing laws

[26] Article 14 of AP2

[27] https://nc4.go.ke/the-computer-misuse-and-cybercrimes-act-2018/

that are established in Kenya are national criminal laws that are municipal in nature. The discussion here is what cyber activities conducted during an armed conflict could constitute violations of IHL and thus be considered offenses. The ICRC considers operations designed to disable computer its self or network as an attack, regardless whether the means are kinetic or cyber. This may include foreseeable indirect effects, such as the loss of life in a hospital due to a cyberattack on the power grid.[28]

Let's not leave the fact that it automatically constitutes as an 'attack' under IHL if it is to violate the fundamental principles, especially the cardinal principle which is to distinguish military objects and the civilian objects and precautions taken to see that the anticipated civilian harm is not excessive in relation to the direct military advantage that will be gained.

3.1.3 Cyber crime and Cyber Security

Kenya's Computer Misuse and Cybercrimes Act of 2018 outlines various penalties for cyber offences.[29] For these offences to be considered as conflict, they have to be persistent from the adversary. If the cyber crimes appear to be APTs, they are then considered conflict under IHL. These crimes however can be validly lawful if only they are a last resort and all other means of including compliance have been exhausted. The maxims of equity apply in that during NIACs reprisals are abled in response to a prior serious violation. Not forgetting limiting the targets to only military objects and against critical civilian objects.

Security in cyber has had concerns about cyber crimes in that legal sectors have created laws that reduce these offences. Criminalizing offenses such as

[28] Cybersecurity Report the National KE-CIRT/CC
[29] The Computer Misuse and Cybercrimes Act, 2018

unauthorized access, cyber espionage, identity theft, cyberterrorism, and cyber harassment. It also facilitates international cooperation in combating cybercrime.[30] Regulating electronic transactions, telecommunications, and cybersecurity measures and a National Computer Incident Response Team (KE-CIRT/CC) to handle cybersecurity threats. [31] This shows that Kenya as a developing state tries to its capacity to keep up with the developing cyber space however, lack the skills to stop such future crimes and stop them from happening. The skills present are those in finding solutions when the threats have happened, the difficulty developing states face.

3.1.4. Ihl and its legal principles

International humanitarian rules and principles derive from international custom that were established in time of armed conflict. IHL being the law of armed conflict provides laws and principles to the parties involved in conflict especially NIACs.[32] Under IHL cyber operations are subject to the same principles that govern traditional warfare, these include, distinction, proportionality, and military necessity thus these attacks should respect civilian and civilian infrastructure during an armed cyber conflict. Any objects indispensable for civilian survival is at all costs prohibited.[33] The dual-use of the digital world between the state and its civilians creates possible outcomes that can challenge Article 14 and 15 of Additional Protocol II.

[30] Computer Misuse and Cybercrimes Act (CMCA) of 2018; https://nc4.go.ke/the-computer-misuse-and-cybercrimes-act-2018/
[31] Kenya Information and Communications Act (KICA); https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/kenya
[32] Common Article 3 of GCs
[33] Article 14 of AP II

3.2 The legal effect of the law of targeting in matters concerning cyber operations

Dams, and nuclear electrical generating stations shall not be made the object of attack, even if they are military objectives.[34] The law of targeting restricts attacks especially in NIACs. In a digital realm, dams and nuclear electrical generating stations extensively use digital technologies in their operations, especially nuclear electrical generating stations that operate with digital technology. Civilians and their objects generally are protected under IHL unless they are to participate in armed cyber conflicts. Even if they are to participate, they are to respect the principles of warfare. Attacks, destruction, demolition of objects indispensable to the survival of the civilian population such as hospitals, foodstuffs, drinking water installations are forbidden.[35] With distinction, cyber attacks must differentiate between military objects and civilian objects. Targeting civilian infrastructure as elaborated above, such as hospitals or water systems, is prohibited unless they are being used for military purposes.[36] And even if the distinction has been proper and there is need to attack, these attacks must be proportionate in that it must not cause excessive harm to civilians and civilian infrastructure. These laws still govern parties in NIACs and should be respected.[37]

3.3 Conclusion

Noting that cyber warfare does not involve physical attack or attacks that are kinetic, attacking civilian infrastructure and its impact on such infrastructure such as, hospitals, power grids, water supply systems and financial institutions can be

[34] Article 15 of AP II
[35] Article 14 of AP II; https://ihl-databases.icrc.org/en/ihl-treaties/apii-1977/article-14
[36] https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law
[37] Common Article 3 of the GCs

severe and a call for IHL. The difficulty to assess damage creates clear lack of attribution. The Tallinn Manual suggests that cyber operations must comply with the existing principles of IHL, but international consensus on specific regulations remains limited.[38]

[38] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
By Andrey L Kozik

Chapter 4

4.0 INTORDUCTION

This chapter entails the summary of findings, conclusions and recommendations. Establishing the threshold in the law of armed conflict under cyber is difficult. Stating whether cyber is an object or not is difficult. This is because IHL recognises violence in the aspect of physical harm, harm that is actual, intended to hurt physically of even kill someone. It may seem impossible and rare for cyber to perform such violence however it is possible and may be connected. Public hospitals and state fall victims in NIACs

4.1. General summary of findings and analysis

The ICRC affirms that IHL applies to cyberoperations during armed conflict, just like the way it applies to traditional warfare.[39] This clearly shows that cyber operations must comply with the principles of IHL especially in the above scenarios of Kenya. With the fact that the digital realm is shared between the society and the state, the principle requires that attacks must only be directed to military objects and not civilian objects.[40] That it amounts to an issue under IHL when cyberoperations target essential civilian services such as water systems, hospitals and power grids.[41]

One of the biggest challenges is attribution when it comes to the aspect of cyber operations in Kenya. Customary international law holds states accountable for

[39] https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf
[40] Article 14 and 15 AP II; https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf
[41] https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf

cyber operations conducted by their military or state-sponsored actors.[42] This also brings challenges in the diplomatic and legal framework. However, the Kenyan municipal laws criminalize cyber attacks and tries to contain them but the direct incorporation of international Humanitarian Law within the municipal laws of Kenya concerning armed cyber conflict appears to be not explicitly stated.

There is need for further legal development is this field. As the ICRC advocates for new laws and treaties, I feel it should be customary for cyber operations in an armed conflict to respect the principles of IHL, there is ongoing debate about whether existing laws are sufficient or if new treaties are needed.[43]

4.2. Recommendations

We can't help the fact that adopting to this new technology to essential services is mandatory. As this development happens, let these developing countries not forget the fact that essential services mostly involve civilians who have to be protected as per the laws of International customary law. Developments have to also happen in the security sector in cyber technologies. These skills of security should foresee the problem before the problem reaches the civilians. African states especially Kenya finds it difficult to further develop skills in security of such an area of technology.

Customary International laws should derive a normative theory that stipulates the protection of civilians and civilian infrastructure during cyber operations in not only International but mainly Non-International armed conflict. There should be an

[42] https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts
[43] https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

effect- based approach, where the impact of civilian and civilian infrastructure determines legality.[44]

There could be an International cooperation. International collaboration where Kenya's legal framework aligns with international norms to effectively regulate cyber operations in armed conflict.[45]

4.3. Conclusion

International customary laws still apply even though the matter is of a NIAC. This is because it is a custom for respect to be given to the Humane aspect of treatment during armed conflict. That parties in an armed conflict are to obey these governing principles to protect civilians and their infrastructure. It has been realised that collaboration within states to create governing laws, find best approach to cyber operation during an armed conflict, as a good way of overcoming such a developing matter. In that it shall become custom for states and non-state actors to follow IHL principles with whatever kind of armed conflict it is; be it cyber or kinetic traditional warfare.

[44] https://www.dlpforum.org/2023/09/06/cyber-operations-falling-under-attack-in-ihl/
[45] https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf

BIBLIOGRAPHY AND LIST OF REFERENCES

STATUTES

- African Union Convention on Cyber Security and personal data protection
- the Rome Statute
- Geneva Conventions
- Computer Misuse and Cybercrimes act 2018 (kenya)
- ICRC AP commentary

BOOKS

- Humanizing the Laws of war edition by detlev F. Vagts by Richard Baxter
- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
- By Andrey L Kozik;

ARTICLES AND REPORTS

- OECD 'Digital Government in Chie – Digital Identity' (OECD Publishing 2019) 7
- M. N. Schmitt and L. Vihul (eds), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
- Cybersecurity Report the National KE-CIRT/CC

WEBSITES AND ONLINE SOURCES

https://dictionary.cambridge.org/dictionary/English/cybercrime/

ICRC, https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf

https://www.cambridge.org/core/journals/american-journal-of-international-law/article/attribution-problem-and-cyber-armed-attacks/

https://unidir.org/publication/non-escalatory-attribution-of-international-cyber-incidents-facts-international-law-and-politics/

https://nc4.go.ke/the-computer-misuse-and-cybercrimes-act-2018/

Computer Misuse and Cybercrimes Act (CMCA) of 2018; https://nc4.go.ke/the-computer-misuse-and-cybercrimes-act-2018/

Kenya Information and Communications Act (KICA); https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/kenya

https://ihl-databases.icrc.org/en/ihl-treaties/apii-1977/article-14

https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law

https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf

https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf

https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf

https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

https://www.dlpforum.org/2023/09/06/cyber-operations-falling-under-attack-in-ihl/

https://www.academia.edu/74844551/Tallinn_Manual_2_0_on_the_International_Law_Applicable_to_Cyber_Operations?auto=download

https://www.kictanet.or.ke/cyberattacks-on-critcal-infrastucture