UNIVERSITY of LUSAKA

Passion for Quality Education: Our Driving Force

SCHOOL OF LAW

(ASSESSING THE EFFECTIVENESS OF INTERNATIONAL HUMANITARIAN LAW IN REGULATING HACKTIVISM IN CYBER WARFARE: A CASE STUDY OF KILLNET)

By:

(JOSEPH ISRAEL BANDA)

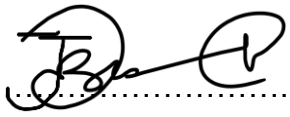
LLB20119811

AN OBLIGATORY ESSAY SUBMITTED TO THE UNIVERSITY OF LUSAKA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE BACHELOR OF LAWS (LLB) DEGREE.

2025

DECLARATION

I, **JOSEPH ISRAEL BANDA**, do hereby declare that this dissertation titled "**ASSESSING THE EFFECTIVENESS OF INTERNATIONAL HUMANITARIAN LAW IN REGGULATING HACKTIVISM IN CYBER WARFARE: A CASE STUDY OF KILLNET**" which is hereby submitted to the School of Law at the University of Lusaka as part of the requirements for the award of the Bachelor of Laws (LLB) degree, is solely of my own and that it has, to the best of my knowledge, not yet been presented for any academic purposes in Zambia or elsewhere. Other people's work and sources used in the study have been acknowledged. I hereby declare that I have read and understood the regulations governing the submission of the Bachelor of Laws Degree (LLB) dissertation including those relating to length and plagiarism, as contained in the rules of the University and that this dissertation conforms to those regulations.

Signature……  ……

Date.....14th.....November.....2025.....

SUPERVISOR'S RECOMMENDATION

I, **JOE MWAULUKA**, do recommend that the dissertation titled '**ASSESSING THE EFFECTIVENESS OF INTERNATIONAL HUMANITARIAN LAW IN REGGULATING HACKTIVISM IN CYBER WARFARE: A CASE STUDY OF KILLNET**' authored by **JOSEPH ISRAEL BANDA**, STUDENT NUMBER LLB20119811 was done under my supervision, be admitted by the University. I have checked it carefully and I am satisfied that it meets the requirements related to format as laid down by the University Regulations governing directed research.

.....

Mr. JOE MWAULUKA

(Supervisor)

……

(Date)

DEDICATION

To my parents, Denis Banda and Regina Laura Banda, whose unwavering support and belief in me were a constant inspiration. Though you are no longer here, your love continues to guide me. To my wife, children, sister and brother your unwavering patience, endless love, and for bearing the extra load without complaining during this long and arduous journey. Your belief in me was my constant motivation.

ACKNOWLEDGEMENTS

First and foremost, I would like to praise and thank God, the Almighty, who has granted me countless blessings, knowledge, and opportunity so that I have been finally able to accomplish this thesis.

I wish to extend my heartfelt gratitude to Mr. Joe Mwauluka my Research supervisor for his unwavering support and guidance throughout the completion of my thesis, your thoughtful feedback and constant encouragement have not only honed my skills but also enriched the quality of this thesis.

I would also like to acknowledge the contribution of my lecturers Mr. Mwika Musakuzi, Ms. V.K Chileshe, Mrs. Milambo Chibbonta Pupwe, Ms. N Mwanamwambwa, Ms. M Chizinga, Ms. L Mwanza, Mrs. K Mwauluka, Mr. J Mulambia and all other University of Lusaka lecturers who shaped my academic life.

To my fellow students David Phiri, Wamundila Kabubi, Paul Chilambwe, Alex Pensulo, Ireen Chanda and Astrida Kaira whose collaborative efforts and wealth of knowledge were unwavering.

This acknowledgment extends to my family and friends whose belief in my abilities and encouragement have provided the emotional sustenance to complete this challenging task.

Table of Contents

ABSTRACT

This thesis assessed the efficacy of International Humanitarian Law (IHL) in regulating hacktivism within cyber warfare both internationally and domestically, specifically analysing the challenges posed by the pro-Russian group Killnet. The study posited that a dual failure in both domains allows groups like Killnet to operate in a significant regulatory void, accelerating humanitarian risks.

Internationally, IHL's core challenge is the legal classification and attribution of Killnet's primary tactic, Distributed Denial of Service (DDoS) attacks against civilian critical infrastructure. The lack of physical injury or destruction from DDoS attacks makes it difficult to classify them as a regulated "attack" under international humanitarian law. Furthermore, Killnet's Self-proclaimed independence, non-state nature and decentralized status severely complicates the establishment of State responsibility and control, creating a clear accountability gap under IHL.

Domestically, the thesis highlighted the failure of many States including Zambia to adequately translate IHL obligations concerning non-state actors into domestic criminal law capable of prosecuting hacktivists for wartime activities. Hacktivists members operate from various global states, making the jurisdictional reach and counter-terrorism laws insufficient for effective enforcement.

The case study of Killnet demonstrated a critical disconnect in line with international humanitarian law. Internationally, IHL struggles with legal definitions and attribution to the state while domestically, national laws lack the necessary mechanisms to consistently prosecute or suppress IHL violations by non-state cyber actors. The thesis concluded that a comprehensive, coordinated effort is required to bridge these international and domestic gaps, including clarifying IHL's application to non-kinetic effects and harmonising domestic legislation to criminalise and enforce the law against hacktivism during armed conflict.

GENERAL INTRODUCTION

CHAPTER ONE

1.0 INTRODUCTION

International Humanitarian Law, also known as the Law of armed conflicts, seeks to limit the effects of armed conflicts for humanitarian reasons. Understanding armed conflicts is vital to understanding this area of Law. International Humanitarian Law is generally defined as the body of international Law that governs the conduct of armed conflicts[1]. Since International Humanitarian Law is concerned with the conduct of armed conflicts, it is therefore important to note that the existence of an armed conflict is a necessary requisite for international Humanitarian Law to function. However, this area of Law is not concerned with whether the use of force is or is not legal, but whether the conduct of the war conforms to the principles of general international law but rather how to conduct war once hostilities break out. Jus in bello, which refers to the principles and rules of international humanitarian law (IHL) that govern the conduct of hostilities during armed conflict, aiming to minimize human suffering are broadly divided into four categories, namely the principle of Humanity, Distinction, proportionality, Necessity and Limitation. International Humanitarian Law principles are backed by the United Nations core treaties, including the Geneva Conventions and Additional Protocols. The Geneva Convention (1949)[2] and their additional protocols form the backbone of international Humanitarian Law, which contains the main protection for individuals in times of armed conflicts. Rules of conduct in armed conflicts have taken a different twist in recent times with advancement of methods of welfare. Traditionally, IHL regulates the conduct of armed conflicts through key areas that include, Prohibition of Attacks Against Civilians, prevention of unnecessary Suffering, treatment of the Wounded and Sick and protection of medical facilities.

---

[1] La Crowe, Jonathan, and Kylie Weston-Scheuber. Principles of International humanitarian Law. Edward Elgar Publishing, 2013. Pg1

[2] Geneva convention International Committee of the Red Cross (ICRC) (1949) Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 12 August 1949, 75 UNTS 287, available at: http://www.refworld.org/docid/3ae6b36d2.html.accessed 16/18/2025.

1.1 BACKGROUND OF STUDY

In recent past, the methods of welfare in armed conflicts have seen drift from conventional methods especially in the advent of advancement of technology. The increase in cyberattacks and cyberwarfare is one that poses huge challenges in international humanitarian law. More typically related to cyber-attacks is Hacktivism, which is a kind of cyberattack that uses computer-based techniques, like hacking, to promote a political or social agenda, often through civil disobedience or raising awareness about specific issues[3]. Hacktivist groups have raised awareness about a wide range of issues, from government wiretapping and internet monitoring to free speech violations. The primary targets of hacktivists are entities such as states, quasi-state actors, and multinational corporations that support the limitations of freedom, including freedom on the internet. Many technologies have caused social and political change and invariably have been used as both tools and weapons in international armed conflicts.[4]

Nowadays, the use of global telecommunications networks has made it easier and cheaper to communicate between businesses, governments and individuals within the quickest possible times. However, these global networks have consequently made it easier for perpetrators of crimes to conduct sophisticated crimes within international networks such as Hacktivism, a convergence of hacking and activism[5]. Hacktivists employ various tactics, including Distributed Denial of Service (DDoS) attacks, website defacement, data leaks, doxxing, and anonymous blogging, to disrupt systems, expose information, and promote their agendas. Within the realm of digital warfare, hacktivist group known as “Killnet” has established itself as a high-visibility force in cyber-attacks whose interest has rapidly grown amidst the Russia-Ukraine war. This highly motivated group has committed distributed denial-of-service (DDos) and data exfiltration attacks against Western entities and Dark Web markets in support of pro kremlin ideologies. While international humanitarian Law has clear objective is limiting effects of “hard war”

[3] https://www.xcitium.com/knowledge-base/hacktivism/#:~:text=In%20an%20era%20where%20digital,influence%20in%20today's%20interconnected%20society. Accessed 17 April 2025

[4] Gawel, H. (2024). Hacktivism. Internet Policy Review, 13(2). https://policyreview.info/glossary/hacktivism accessed 17 April 2025

[5] Samuel, Alexandra Whitney. *Hacktivism and the future of political participation*. Harvard University, 2004.

armed conflict, there is a huge task that arises when dealing with “soft wars” like hacktivism and cyberwar attacks due to several factors. These factors may include Lack of Clear Legal Classification of Hacktivists, difficulties in Enforcement of cyber operations due to lack of jurisdiction and attribution issues which make Sit difficult to tell whether a cyber-attack originates from an individual, a non-state group, or a state-backed entity and finally the gaps in the law. Clearly, there is urgent need to ensure that the emergency of soft wars that poses the same threats to conventional effects of armed conflicts are dealt with decisively under the International Humanitarian Law.

1.2 STATEMENT OF PROBLEM

The 1949 Geneva Convention and its optional protocols form the core of International Humanitarian Law, whose aim is to limit the suffering of people affected by armed conflicts including those who are no longer fighting and civilians.

Despite the International Humanitarian Law principles that mitigate the effects of armed conflicts, such as protecting those who are no longer involved in hostilities and ensuring that attacks are directed at legitimate targets or limitation on the methods of warfare to prevent unnecessary suffering, there are a lot of challenges in limiting the effects posed by cyber-attacks or hacktivists in armed conflicts under IHL.

In line with these challenges, investigating the effectiveness of international humanitarian law in regulating Hacktivism in armed conflicts is crucial in upholding the general principles of international humanitarian law which is the focus of this research.

It is important that in the advent of technological advances, hacktivism and cyberwarfare is fully addressed under international humanitarian law to brace for both current and future conflicts.

1.3 GENERAL OBJECTIVES

The study aims at assessing the effectiveness of the international humanitarian Law (IHL) in regulating hacktivism in cyber warfare

1.3.1 SPECIFIC OBJECTIVES

The following are the specific research objectives:

i. To critically assess the legal framework on International Humanitarian Law and examine the core treaties under IHL that relate to hacktivism and cyber warfare.

ii. To critically examine the role of International Humanitarian Law and cybersecurity frameworks in combating hacktivism and cyber warfare.

iii. To examine the challenges of applying International Humanitarian Law to counteract hacktivism threats.

1.4 RESEARCH QUESTIONS

The study will cover the following questions.

i. What is the legal framework on International Humanitarian Law and the core treaties under IHL that relate to hacktivism and cyber warfare?
ii. What is the role of International Humanitarian Law and cybersecurity frameworks in combating hacktivism and cyber warfare?
iii. What are the challenges of applying International Humanitarian Law to counteract hacktivism threats?

1.4 SIGNIFICANCE OF STUDY

This research will seek to uncover issues surrounding application of international humanitarian Law principles in the wake of increased technology and cyber warfare. The aim of this research is to address the current and future effects that hacktivism and cyber warfare possess to armed conflicts under international Humanitarian Law. The research will endeavor to add to existing knowledge in the application of International Humanitarian Law principles in combating conflicts related to cyber warfare.

1.6 SCOPE OF STUDY

The area of study is countries primarily impacted by cyber-attacks with specific focus hacktivist group '**Killnet**'. The research will also review existing Cybersecurity Laws that regulate cyber activities in Zambia. In attempting to accomplish this, the study will refer to various specific international law instruments like **1949 Geneva Convention**[6], **Tallinn Manual**[7], **Responsibility of States for Internationally Wrongful Acts**[8], **The Cyber Crimes Act**[9] and **The Cyber Security Act**[10], cases law and scholarly works relating to the similar topic in contention.

1.7 LITERATURE REVIEW

Traditionally international humanitarian law is based on elements of military necessity and humanity that aims to allow the use of force to achieve a legitimate objective but also humanity to prohibit unnecessary suffering and destruction. A review on the effectiveness of the international humanitarian law in regulating hacktivism in cyber warfare was undertaken.

---

[6] The Geneva Convention 1949

[7] Schmitt, Michael N., ed. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 2017.

[8] Responsibility of States for Internationally Wrongful Acts 2001

[9] Act No 4 of 2025

[10] Act No 3 of 2025

Halme-Tuomisaari, Miia[11] "International Humanitarian Law (IHL) can be classified under two distinct trajectories, namely the Hague Conventions and the Geneva Conventions. Each term refers to a cluster of treaties and declarations while also having distinct emphasis: the Hague Conventions articulate acceptable methods of warfare, conduct of hostilities, and occupation, while the Geneva Conventions are directed at protecting the individual, civilians during warfare as well as injured combatants. According to these conventions, international humanitarian law (IHL) prohibits means and methods of warfare that cause superfluous injury or unnecessary suffering. As a result, certain types of weapons are not allowed, and the way other weapons are used is restricted". This research, however, focuses on the interpretation of Geneva convention regarding cyber-crimes as a method and means of warfare and how it impacts those in conflict zones which this literature review does not cover.

The 1949 Geneva Convention, Additional Protocol I, specifically Articles 48, 51, and 52, emphasizes the principle of distinction. This principle requires parties to an armed conflict to always distinguish between civilians and combatants, and between civilian objects and military objectives. The research further examines the interpretation of this provision as to the nature of hacktivist in relation to the principle of distinction and how IHL classifies them.

Dinstein, Yoram[12] "Under humanitarian law, all persons who are not or no longer taking part in hostilities are protected. In the context of international armed conflicts, they are referred to as "protected persons," but they benefit from protection under humanitarian law in non-international conflicts as well. The Geneva Conventions make a distinction between several categories of persons: the wounded and sick (whether military or civilian), prisoners of war, interned or detained civilians, and civilians in occupied or enemy territory. All individuals must be treated humanely. Each category of person benefits from a general regime of protection, which is specifically adapted to their situation. Fundamental guarantees are also provided as a minimum to all persons". The

[11] Halme-Tuomisaari, Miia. "International Humanitarian Law." *Humanitarianism: Keywords*, edited by Antonio De Lauri, Brill, 2020, pp. 120–22. *JSTOR*, http://www.jstor.org/stable/10.1163/j.ctv2gjwwnw. Accessed 12 Apr. 2025

[12] Dinstein, Yoram. *The Conduct of Hostilities under the Law of International Armed Conflict* . Cambridge: Cambridge University Press, 2004

researcher's work, however, departs from the literature reviewed in that it, although the author makes a distinction as to which persons are classified as non-combatants, he does not state how hacktivists are classified under international humanitarian law.

Gisel, Laurent, Tilman Rodenhäuser, and Knut Dörmann[13] "The conclusion that IHL applies to cyber operations during armed conflict finds further support in the views expressed by the ICJ. In its Advisory Opinion on the legality of the threat or use of nuclear weapons, the Court recalled that the established principles and rules of humanitarian law applicable in armed conflict apply "to all forms of warfare and to all kinds of weapons", including "those of the future"'." While this research supports in part the author's view that IHL applies to cyber operations, the researcher further examines the basis of supporting this preposition and highlights challenges in applying this law to cyber operations,

Dixon, Martin, Robert McCorquodale, and Sarah Williams[14] "rules of State responsibility are codified under the international Law commission which asserts that State responsibility arises from the violation by a State (or other international legal person) of an international obligation".

James D. Fry[15] According to the International Law Commission (ILC) Commentary to the ARSIWA, attribution of conduct should be determined by international law rather than by causality, making it a normative operation. In accordance with the law of State responsibility, every internationally wrongful act gives rise to the liability of the State that caused it. Internationally wrongful conduct consists of an action or omission: (a)'attributable to the State under international law' and (b) constitutes a breach of an international obligation of the State' (Art 2 ASR). As a departure from the literature

[13] Gisel, Laurent, Tilman Rodenhäuser, and Knut Dörmann. "Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts." *https://international-review.icrc.org/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber-913* accessed 18 April 2025

[14] Dixon, Martin, Robert McCorquodale, and Sarah Williams. *Cases and materials on international law*. Oxford University Press, USA, 2011. Pg462

[15] Fry, James D. "Attribution of responsibility." Principles of shared responsibility in international law: An appraisal of the state of the art (2014)

reviewed, the researcher examines the interpretation of ILC articles on the responsibility of states when applied to hacktivism and cyber operations under international law.

Laurent Gisel, Tilman Rodenhäuser, and Knut Dörmann[16] "In the use of information and communications technologies, the principle of distinction requires that parties to an armed conflict always distinguish between civilians and combatants and between civilian objects and military objectives. Cyber-attacks may only be directed against combatants or military objectives. Cyber-attacks must not be directed against civilians or civilian objects. Indiscriminate cyber-attacks are prohibited". Although like the author's, the researcher acknowledges that to address the challenges in applying IHL to Hacktivism the principle of distinction must apply, however, in departure from this review, the researcher further explores how this distinction is applied and other aspects of mitigating challenges faced with cyber warfare in international Law.

Eiton Diamond[17] "The difficulty of adapting IHL to cyber warfare is compounded by the veil of secrecy enveloping cyber security operations. Law, after all, must be applied to facts. When the facts are not well known it is not possible to have clear legal reading. More precisely, key information needed in order to make an informed evaluation of cyber operations compatibility with IHL is often lacking, including details about (a) the technology available, (b) the attacks conducted, (c) the identity of the parties conducting the attacks, and (d) the policies, guidelines, and rules that states apply in relation to cyber warfare, along with their reading of the applicable rules of IHL. Information about the technological capabilities that exist or are under development is necessary to evaluate whether the methods and means of warfare facilitated by these technologies meet the requirements of IHL".

Like the author in this literature review, the researcher acknowledges that to address the challenges in applying IHL to cyber warfare, the task demands collaborative efforts of

[16] The Principle of Distinction: Cyber Operations During Armed Conflict" international committee for the Red Cross. https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf accessed 20 April 2025

[17] Eitan Diamond, 'Applying International Humanitarian Law to Cyber Warfare', Law and National Security: Selected Issues, Containing: Applying International Humanitarian Law to Cyber Warfare https://www.jstor.org/stable/pdf/resrep08957.8.pdf accessed April 20, 2025

policymakers, legal experts, and the global community. Core principles of IHL, including the principle of distinction, stand as collective commitment to preserving humanity in the face of the ever-advancing frontiers of warfare. Furthermore, enhancing cybersecurity education and awareness is a fundamental step toward strengthening the application of the principle of distinction in cyber warfare. By equipping both military and civilian stakeholders with knowledge and tools to navigate the complexities of cyberspace, it is possible to promote compliance with IHL. The researcher, however, departs from this review by addressing the challenges faced in applying IHL to Hacktivism in regard to the core principles of IHL, cybersecurity education, stakeholder involvement and clear understanding of key terms as 'attack' in application of hacktivism is essential under international humanitarian law.

1.8 METHODOLOGY

1.8.1 RESEARCH APPROACH

This research will employ qualitative research methodology. Taking an analytical approach, the research will examine, evaluate, and critique existing legislation, judicial decisions, books, articles, journals and other scholarly works. Information will be sourced from both primary and secondary sources mentioned above**.**

1.8.2 RESEARCH DESIGN

The research will adopt an integrated approach, primarily focusing on library as well as desk research for data collection, and the data analysis process entails a critical and thorough review and description of applicable legal provisions**.**

1.8.3 SAMPLE SIZE This research will be targeted at all people with credible knowledge and expertise on the subject matter.

1.8.4 SAMPLING TECHNIQUE This research employed a Judgmental technique as well as the snowball technique with the aim of obtaining the most accurate and credible up to

date information from reliable and trustworthy institutions and experts.

1.8.5 ETHICAL CONSIDERATION

The author shall endeavor during this research to abide by ethical principles in order not to violate any written law and/or breach any individual's rights to privacy. To adhere to ethical requirements, prior consent shall be requested from individuals or organizations willing to participate in the study as well as from the University of Lusaka ethics committee. Further, to conform with ethical requirements of research, first permission will be sought from the UNILUS research ethics committee, second, permission will be sought from organizations, third, permission will be sought from individual research subject, lastly, researchers will endeavor to follow academic writing requirements like referencing and acknowledgement of other people's work.

1.9 RESEARCH OUTLINE

CHAPTER ONE sets out the introduction for this research, it introduces the research topic and discusses the statement of problem, literature reviews, the significance of the study and the research methodologies used to achieve the objective of the research.

CHAPTER TWO focuses on examining core treaties of International Humanitarian Law, including Additional Protocols, and Tallinn Manual 2.0 on Cyber Warfare, examining how IHL applies to cyber operations. The chapter also examines how IHL classifies hacktivists under the principles of IHL and investigates how state responsibility applies to hacktivists and cyber operations and explores cases where cyber warfare or hacktivism has been addressed in legal rulings or international discussions

CHAPTER THREE will examine the Role of International Law and Cybersecurity frameworks and policies States have implemented to counteract hacktivism and cyberwarfare threats while complying with International Humanitarian Law. Zambia's legal framework in regulating cyber activities and how they align with international standards.

CHAPTER FOUR will focus on Challenges in Applying International Humanitarian Law to Hacktivism, the difficulties in Enforcement, attributions issues and gaps in the law, Domestic challenges. Draw distinctions between hacktivist groups from cybercriminals and state-sponsored actors, further undertaking a case study of **Killnet** their history, motivation, cyber-attacks and how affected States and international organizations have responded to these cyber-attacks under international Humanitarian Law

CHAPTER FIVE Summarizes the preceding chapters and additionally, provides recommendations that will aid in addressing the legal challenges identified in the research.

CHAPTER TWO

ASSESSMENT OF THE LEGAL FRAMEWORK ON INTERNATIONAL HUMANITARIAN LAW AND EXAMINATION OF THE CORE TREATIES UNDER INTERNATIONAL HUMANITARIAN LAW AND HOW THEY RELATE TO HACTIVISM AND CYBER WARFARE

2.0 INTRODUCTION

This chapter will undertake an assessment of the legal framework on International Humanitarian Law and examine the core treaties under IHL that relate to hacktivism and cyber warfare. This will be done by analyzing the provisions of the legal and institutional framework that governs international humanitarian Law and how they apply in armed conflicts. This chapter will also elaborate whether these provisions apply to hacktivism and cyberwarfare. Eventually a conclusion shall be drawn from the analysis.

2.1 LEGAL FRAMEWORK OF INTERNATIONAL HUMANITARIAN LAW

The legal framework of International Humanitarian Law (IHL), also known as the law of armed conflict or *jus in bello*, is predominantly coined to limit the effects of armed conflict for humanitarian reasons. This body of international law is drawn from two primary sources: the codified rules found in international treaties and the uncodified rules of customary international law. The four **Geneva Conventions of 1949** and their Additional Protocols form the backbone of the treaty law, universally adopted by States to ensure humane treatment in wartime. Consequently, all States have an obligation to respect and ensure respect for IHL, making it a critical aspect of international jurisprudence and global security

2.1.1 THE GENEVA CONVENTION (1949)

The Geneva conventions of 1949 and their additional protocols form one of the key fundamental sources of international humanitarian law, which is an international body of rules that limits the effects of armed conflicts. The convention is a collection of four separate conventions, each having a distinct application to the main objective. The first convention regarded as **Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field** is aimed at protection of wounded and sick in armed conflicts and for medical and religious personnel, medical units and medical transports[18]. The second convention, known at **Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea,** has its focus on the protection of wounded, sick and shipwrecked members of armed forces at sea, these articles provide specific protection for hospital ships, coastal rescue craft, medical aircraft and other medical transports at sea, as well as religious, medical and hospital personnel performing their duties in a naval[19]. The third convention is the **Convention (III), relative to the Treatment of Prisoners of War aims at ensuring that equal treatment is granted to prisoners of war**. This Convention establishes the principle that prisoners of war must be released and repatriated without delay after the cessation of active hostilities[20]. Lastly **Convention (IV) relative to the Protection of Civilian Persons in Time of War** provides for vital protection for civilians in occupied territories and other areas, ensuring their safety, humanitarian relief, and protection from harm.

As an expansion to the Geneva Conventions 1949, there are three distinct additional protocols that supplement the objectives of the main convention in regulating armed conflicts. The first additional protocol, **Protocol Additional to the Geneva Conventions**

[18] ICRC Database, **Treaties, States Parties and Commentaries**, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949., https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949 accessed 7 August 2025

[19] ICRC Database, **Treaties, States Parties and Commentaries**, Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. Geneva, 12 August 1949., https://ihl-databases.icrc.org/en/ihl-treaties/gcii-1949 accessed 7 August 2025

[20] ICRC Database, **Treaties, States Parties and Commentaries**, Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949., https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949 accessed

of 1949 and relating to the Protection of Victims of International Armed Conflicts, Contains fundamental guarantees for people not taking part in hostilities during an international armed conflict and sets forth rules on protecting civilians, civilian objects and the installations essential for civilians' survival[21]. The additional protocol II mainly referred to **Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts**, contains fundamental guarantees for people not taking part in hostilities during non-international armed conflicts and sets forth rules on protecting civilian objects and the installations essential for civilians' survival. The third protocol, **Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Adoption of an Additional Distinctive Emblem** established the additional emblem alongside the existing emblem to distinctly identify and provide protection to medical and religious personnel and facilities during armed conflicts[22].

2.1.2 CUSTOMARY INTERNATIONAL HUMAITARIAN LAW

"International humanitarian law has its origins in the customary practices of armies as they developed over the ages and on all continents."[23]

Customary international humanitarian law provides for the protection of victims of war including horse de combat, civilians and prisoners by ensuring that they are treated humanely regardless of whether a treaty applies or not. It also prohibits the weapons and methods used in welfare that tend to cause superfluous injury, unnecessary suffering or fail to distinguish between civilians and combatants. Where no formal treaties exist, especially in non-international armed conflicts, Customary international humanitarian law steps in to provide binding rules on parties to an armed conflict[24]. There are several rules on which customary international humanitarian Law draw its legal binding authority. This chapter will highlight some of the important rules.

[21] International Humanitarian Law Handbook for Parliamentarians N° 25, pg13
[22] Ibid,p14
[23] Jean-Marie Henckaerts and Louise Doswald-Beck 'Customary International Humanitarian Law Volume 1(2005), Cambridge university press, p32.
[24] Ibid p39

The principle of distinction forms the cornerstone of customary international humanitarian law and aims to ensure that parties to the conflict must always distinguish between civilians and combatants. Attacks may only be directed against combatants and must not be directed against civilians[25]. Established under State practice, this rule applies to both non-international and international conflicts and requires that parties to an armed conflict are obliged and bound to distinguish between those members of the armed forces or organized armed groups who are legally entitled to participate directly in hostilities and those that are not legally permitted to participate directly in armed conflicts. The principle of distinction is also outlined in **article 47 of the additional protocol 1**[26]. Israel's Military Court at Ramallah recognized the immunity of civilians from direct attack as one of the basic rules of international humanitarian law[27].

The other important rule of customary international humanitarian law relates to acts or threats of violence, the primary purpose of which is to spread terror among the civilian population is prohibited. This rule established under State practice as a norm of customary international humanitarian law also backed by **Article 52 of the additional protocol I** prohibit violence or threats that primarily bring about terror civilian population. This rule does not only apply to States that are party to the Additional protocol I but also those States that are not, as applied under customary international Law. Article 33 of the Fourth Geneva Convention prohibits such acts as terrorism, pillage, and reprisals against protected persons and their property[28]. Violation of such rules in any armed conflicts either non-international or international conflict, is an offence under a lot of legislation in many States. Arguably, the indictments in the Dukic case, Karadzic and ´ Mladic case and Galic case before the International Criminal Tribunal for the Former Yugoslavia included charges of terrorising the civilian population in violation of the laws and customs

[25] Ibid p69

[26] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, 1125 UNTS 3

[27] The Military Prosecutor V Omar Mahmud Kassem and Others (1969)

[28] Convention (IV) relative to the Protection of Civilian Persons in Time of War, Geneva, 12 August 1949, 75 UNTS 287

of war shows the consequences that emanates from abrogation of this rule[29].

According to customary international humanitarian law, State practices establish that under rule 3, All members of the armed forces of a party to the conflict are combatants, except medical and religious personnel. While combatants are clearly defined in international armed conflicts, they are not clearly defined under non-international armed conflicts. Both customary international humanitarian law and treaty provisions have tried to classify 'fighters' as combatants, which many State actors do not agree with.

State practice establishes rule 54 as a norm of customary international humanitarian law in both international and non-international armed conflicts and prohibit Attacking, destroying, removing or rendering useless objects indispensable to the survival of the civilian population are prohibited. Under international conflicts, article 54(2) of the additional protocol (1) specifically prohibits attacks that accelerate starvation of the civilian population. Many military manuals supported by most States prohibits attack in non-international conflicts that attacking objects indispensable to the survival of the civilian population is an offence under the legislation of several States[30]. Additional Protocols I and II provide the following examples of objects indispensable to the survival of the civilian population: foodstuffs, agricultural areas to produce foodstuffs, crops, livestock, drinking water installations and supplies, and irrigation works[31].

Customary international humanitarian Law provides for the principles regarding the use of weapons. Specifically, State practice establishes as a customary international law, that the use of means and methods of warfare which are of a nature to cause superfluous injury or unnecessary suffering is prohibited both in non-international and international conflicts[32]. The prohibition of the means of warfare which are of nature to cause superfluous injury, or unnecessary suffering refers to the effect of a weapon on

[29] Jean-Marie Henckaerts and Louise Doswald-Beck 'Customary International Humanitarian Law Volume 1(2005), Cambridge university press P71

[30] Agreement on the Application of IHL between the Parties to the Conflict in Bosnia and Herzegovina, para. 2.5

[31] Jean-Marie Henckaerts and Louise Doswald-Beck 'Customary International Humanitarian Law Volume 1(2005), Cambridge university press P254

[32] Ibid p298

combatants[33]. In its advisory opinion in the Nuclear Weapons case, the International Court of Justice defined unnecessary suffering as “a harm greater than that unavoidable to achieve legitimate military objectives”.

The following weapons have been cited in practice as causing unnecessary suffering if used in certain or all contexts: lances or spears with a barbed head, serrated-edged bayonets; expanding bullets; explosive bullets; poison and poisoned weapons, including projectiles smeared with substances that inflame wounds; biological and chemical weapons; weapons that primarily injure by fragments not detectable by X-ray, including projectiles filled with broken glass; certain booby-traps; anti-personnel landmines; torpedoes without self-destruction mechanisms; incendiary weapons; blinding laser weapons and nuclear weapons.

2.2 HOW THE LEGAL FRAMEWORK IN INTERNATIONAL HUMANITARIAN LAW RELATE TO HACTIVISM AND CYBER WARFARE

The means and methods of welfare have relatively remained unchanged for centuries and the application of principles of international humanitarian law have not changed drastically. However, the technological advancement in the way wars are fought a drastic shift from conventional welfare has created challenges in the rules and principles of international humanitarian law.

2.2.1 APPLICATION OF INTERNATIONAL HUMANITARIAN LAW TO CYBER WARFARE

International Committee of Red Cross (ICRC) defines cyber warfare as ‘Any hostile measures against an enemy designed to discover, alter, destroy, disrupt or transfer data stored in a computer, manipulated by a computer or transmitted through a computer.’[34]Cyber warfare is also defined as ‘The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information

[33] Ibid p299

[34] International Committee of the Red Cross, ‘Cyber Warfare’ https://www.icrc.org/en/document/cyber-warfare> accessed 9 August 2025

systems for strategic or military purposes'[35]. One of the fundamental principles of internation humanitarian law is the application of the principle of distinction, which requires parties to an armed conflict to distinguish between combatants and non-combatants in international humanitarian law and that military attacks ought to be directed to legitimate targets. Cyber warfare meets the term 'attack' under international humanitarian law, as any conduct initiated in or through cyberspace that is designed or can be reasonably expected to cause injury or death to persons or damage or destruction to objects. In both international and non-international armed conflicts, violation of the principle of distinction that causes human suffering, and humanitarian crisis may lead to State responsibility under war crimes tried at international and national courts. From this principle, cyber warfare that leads to attacks classified under international humanitarian law has the same consequences as those committed under traditional warfare.

The other principal rule of international humanitarian Law, is the principle of proportionality, relating to acts or threats of violence whose primary purpose is to spread terror among the civilian population. International customary law as highlighted earlier, prohibits violence or threats that primarily bring about terror to civilian population. In case of cyber warfare, any acts of violence that bring about adverse suffering to humanity are a violation of international humanitarian law. According to Tallinn Manual 2.0[36], cyber operations attributable to a State which lead to physical effects and harm in the territory of another State constitute a violation of that State's territorial sovereignty and against the international humanitarian law.

In line with the means and methods of warfare which are of a nature, that cause superfluous injury or unnecessary suffering in both non-international and international conflicts, IHL prohibits such weapons. While customary international humanitarian law lists several weapons and means of warfare that are prohibited in traditional warfare, there is no classification on the types of weapons that are prohibited in cyber warfare. However, in reliance on customary international law and established by State practices,

[35] 'Oxford Dictionary', https://en.oxforddictionaries.com/definition/cyberwarfare accessed 9 August 2025

[36] Schmitt, Michael N., ed. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, 2017, Rule 4, para. 11.

any attack that falls within the classification of 'attack' under IHL regardless to whether applied by traditional warfare or cyber warfare remain prohibited.

2.2.2 APPLICATION OF INTERNATIONAL HUMANITARIAN LAW TO HACKTIVISM

Hacktivism is a combination of two words 'Hack' and 'Activism', which is the act of breaking or hacking computer systems driven by political or social motives. International humanitarian Law seeks to limit the effects of armed conflicts by humanitarian reasons by protecting people who are or no longer participation the conflict and limits the means and methods of warfare[37]. Under IHL, assessing the existence of an armed conflict determines whether rules of international humanitarian law will apply or not. In the case of Hacktivism, the classification of whether such attacks amount to armed conflict is therefore important.

According to the ICRC, "to determine when IHL applies to cyber operations between two or more States it must be differentiated that, firstly where a cyber operation is carried out by one State against another in conjunction with or in support of classic 'physical' or 'kinetic' military operations in the context of an existing armed conflict, IHL applies to such operations. Secondly if outside an existing armed conflict, cyber operation is the only means by which hostile actions are undertaken by one State against another State, the law is unsettled as to whether such cyber operation could bring into existence an international armed conflict as defined under Article 2 common to the Geneva Conventions"[38]. Where a hacktivist who are non-State actors conduct cyber operations that potentially damage critical infrastructure that may not amount to non-international armed conflict and may not be subject to rules of international humanitarian law accordingly.

[37] ICRC, Advisory Service On international humanitarian Law http://www.icrc.org/ https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/what_is_ihl.pdf accessed 11 August 2025

[38] Cyber Operations During Armed Conflict https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/01_when_does_ihl_apply-0.pdf accessed 11 August 2025

The principle of military necessity is the hallmark of international humanitarian Law and its application to hacktivism is of utmost importance. The International Court of Justice points out that IHL is designed in such ways that it applies 'to all forms of warfare and to all kinds of weapons, including 'those of the future'[39]. There is no exhaustive list of what forms of warfare should apply under IHL. These may include any kind of warfare both current and those of the future.

2.4. CONCLUSION

The chapter has endeavored to highlight the legal framework the govern international humanitarian law and whether the rules and principles apply to cyber warfare and hacktivism. The IHL draws its system of laws, regulations, policies and legal principles from the international specific conventions, treaties and customary international law. The main. The Genena Conventions 1949 with its additional protocols is the primary source of international humanitarian law that ensures that parties to armed conflicts adheres to all the underlying principles of IHL.

The other sources of rules and principles of IHL are drawn from customary international humanitarian practices that States have established collectively over time. Customary international humanitarian Law supplements the other core treaties by upholding the principles of distinction, precaution, proportionality, humanity and military necessity. It may be said that despite the advancement of modern technology in how armed conflicts are conducted, the rules and principles of IHL drawn from both conventions and customary international Law still apply to a larger extent in cases of hacktivism and cyber warfare.

[39] International Court Of Justice, 'Legality of the Threat or Use of nuclear weapons, Advisory Opinion', (1996), para. 86

CHAPTER THREE

THE ROLE OF INTERNATIONAL HUMANITRIAN LAW AND CYBERSECURITY FRAMEWORK IN COMBATING HACTIVISM AND CYBER WARFARE

3.0 INTRODUCTION

This chapter will focus on the role of international humanitarian Law and cybersecurity frameworks and various policies States have implemented to counteract hacktivism and cyber warfare threats while complying with International Humanitarian Law. The chapter further outlines, Zambia's legal framework in regulating cyber activities, legislative advancements and alignment with international standards.

3.1 INTERNATIONAL HUNAMITARIAN LAW AND CYBERSECURITY FRAMEWORK

The legal framework of international humanitarian law is modeled on two important sources: treaties and customary international law. Even though there are many international cybersecurity frameworks, there are three key international cybersecurity frameworks which include the ISO/IEC 27001, NIST Cybersecurity Framework and the Center for Internet Security (CIS) Controls which provides overarching guidance in security controls and best practices.

3.1.1 INTERNATIONAL HUMANITARIAN LAW LEGAL FRAMEWORK

Whilst the application of international Humanitarian Legal framework in conventional warfare is direct, its application in cyberwarfare is both direct and indirect. Firstly, for IHL framework to apply to hacktivism and cyberwarfare, the attack ought to have a level of IHL violation in the context of armed conflict and cause significant harm to civilians and civilian objects. According to the ICRC[40], An armed conflict arises whenever there is fighting between States or protracted armed violence between government authorities and organized armed groups

[40] ICRC The Law of armed conflict, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/law1_final.pdf. Accessed 03.09.25

or just between organized armed groups. The existence of an armed conflict maybe be classified as international armed conflict or non-international armed conflict. Secondly, hacktivism and cyber warfare should conform to the principles of distinction, proportionality and precaution to be classified as a violation under IHL.

The international Humanitarian Law is not codified into a single document but rather draws its legal force from treaties in addition to customary international law that forms the primary legal framework in international humanitarian law. Conventionally, the IHL legal framework's role is to limit suffering during armed conflicts by protecting non-combatants, regulating the means and methods of warfare, and ensuring humane treatment for those who have ceased fighting. Treaties like the **Geneva Conventions of 1949 and their Additional Protocols** form the core of International Humanitarian Law (IHL). However, in the context of cybersecurity, there is no single global cyber treaty that binds all member states. Bilateral and regional agreements such as the **Council of Europe's Budapest Convention on Cybercrime**[41] serve as frameworks for cooperation and shared legal standards. The main objective of the Council of Europe's Budapest Convention on Cybercrime is provided in Article 23[42] which among others is to criminalize cybercrimes, provide for procedural powers to investigate these crimes and secure digital evidence through member state co-operation to combat them. This framework aims to protect society from cybercrimes by providing a common strategy for member states to take action against offenses like illegal access, data interference, fraud, and child pornography.

According to the Convention on Cybercrime explanatory report, the convention aims primarily at, harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime, providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form and setting up a fast and effective regime of international co-operation[43]. Article 37 of the same convention allows for accession to the convention by non-European union Sates aside from those withing the region. Some of

[41]The Convention on Cybercrime (ETS No. 185)

[42] ibid

[43] https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf. Accessed 11 October 2025

the non-EU member states include, Brazil, United States of America, Nigeria, Ghana, Kenya among others.

Like the Council of Europe's Budapest Convention on Cybercrime, the **African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention)**[44] objectives are aimed at protecting institutions and individuals from cyber threats and privacy violations, combat cybercrime, and establish a legal and institutional framework for cybersecurity and data protection. However, contrary to the Council of Europe's Budapest Convention on Cybercrime**,** African Union Convention on Cyber Security and Personal Data Protection in Article 35 does not allow membership from other non-African Union member States to accede to the convention. This has been seen as a drawback by some scholars in the global fight against cyber crimes

Chapter III of the Malabo convention specifically aims at promoting cybersecurity and combating cybercrimes within member States. Through national policy, the convention outlines the need for each Member State to develop, in collaboration with stakeholders, a national cyber security policy which recognizes the importance of Critical Information Infrastructure and identifies the risks facing the nation in line with cyber security threats[45].

Recently, the United Nations General Assembly, through a proposal made by Russia in 2017, adopted the **United Nations Convention against Cybercrime**, a global treaty aimed at strengthening international cooperation to combat cybercrime and protecting societies from digital threats. According to the UN Secretary General Antionio Guterres, "*This treaty is a demonstration of multilateralism succeeding during difficult times and reflects the collective will of Member States to promote international cooperation to prevent and combat cybercrime*"**[46]** Article 1[47] of the convention provides a layout of the purpose of the treaty which includes; Promotion and strengthening measures to prevent and combat cybercrime more efficiently and effectively, Promote, facilitate and strengthen international cooperation in preventing and combating cybercrime; and Promote, facilitate and support technical assistance and capacity-building to prevent and combat

[44] African Union Convention on Cyber Security and Personal Data Protection, 2014
[45] Ibid, Article 24
[46] https://news.un.org/en/story/2024/12/1158521 accessed 12.10.25
[47] United Nations Convention against Cybercrime 2024

cybercrime, in particular for the benefit of developing countries.

3.1.2 CYBERSECURITY FRAMEWORK

International Law provides for the protection of both State and Non-State actors. Non-State actors such as multinational corporations and Non-governmental Organizations (NGOs) need to adopt advanced and reliable cybersecurity measures to counteract threats posed by hacktivists. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) often referred to as ISO/IEC 27001 is an information security management standard (ISMS) framework adopted by tens of thousands of organizations which include government agencies, NGOs, technology companies, and businesses[48]. The ISO/IEC 27001 provides a model for establishing, maintaining, operating, reviewing and improving information security systems. By conforming to this standard, organizations agree to comply by putting in place a security system that will manage any risk related to security of data they handle[49]. With the increasing number of cyber attacks and crimes, it would be virtually impossible for organizations to manage these risks without a security standard like ISO/IEC 27001.

According to clauses 4 of the ISO/IEC 27001, in understanding the needs and expectations of interested parties, the organization shall determine:

a) interested parties that are relevant to the information security management system. Clause 6 provides for actions that are required to address risks and opportunities. Its entails that "When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s)"[50]. Where there is need to identify parties that may be targets of possible cyber threats in armed conflict, organizations under the ISO/IEC 2700 may classify such parties and determine the risks and opportunities that may require to be addressed to ensure limitations of effects of such attacks.

[48] International Organization for Standardization (ISO/IEC 27001:2022)
[49] ibid
[50] Ibid clause 6

The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks[51]. The Cybersecurity Framework (CSF) is designed to help any organization whether it's a government agency or non-profit organization to manage and reduce cyber risks. The CSF is based of six core functions which include, to govern, identify, protect, Detect, Respond and Recover which are designed to provide a comprehensive approach to the management and reduction of cyber risks[52]. The Gover Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in case of risks. The Identify and Protect functions allow the organization to understand its cybersecurity risks and safeguard the assets are risks identified respectively. Once identified and protected, the 'detect' function then analyses the possible cybersecurity attacks and compromises by timely discovery and analysis of anomalies. The Respond and Analyse Functions requires taking actions and restoration of assets by cybersecurity incidents respectively.

The Center for Internet Security (CIS) Controls is another widely adopted cybersecurity framework. The CIS is aimed at ensuring controls and best practices that enhances organizations and State agencies to strengthen their defenses against cyber threats. Based on three tier approaches, the CIS first identifies the environment to ensure what is to be protected. This may include the critical data and software with potential to result in serious harm once attacked. Then, the CIS framework having identified the environment will ensure that all important assets are protected through risk management improvements. This is done through structured step-by-step processes to identify, assess, and manage risks. Lastly, preparation against attack through incidence response plans, backup and IT cybersecurity experts.

From the foregoing, both the international humanitarian Law framework and cybersecurity framework, although different in the sense that, IHL framework provide rules to mitigate harm during armed conflict while the cybersecurity framework establishes preventative measures, incident response, and legal accountability for cyber activities they complement each other in view of minimizing effects of hacktivism and cyber warfare.

IHL prohibits cyber operations that tend to cause long term destruction to civilian

[51] NIST Cybersecurity framework

[52] Ibid page3

infrastructure such as power plants or water systems or directly harm civilians.

It establishes rules for the conduct of hostilities in cyberspace, requiring parties to distinguish between civilian and military targets and to take precautions to avoid civilian casualties[53].

National and international cybersecurity strategies aim to develop strong defenses and cyber capacities to prevent attacks from occurring in the first place.

Frameworks include mechanisms for capturing threat information, sharing incident data, and promoting public awareness and professional training to enhance cybersecurity knowledge and preparedness. Consequently, Cybersecurity laws criminalize unauthorized access to computer systems and data, providing tools to hold perpetrators accountable for their actions under domestic and international laws. These measures, if applied under IHL, may limit the effects of cyber operations during armed conflicts.

3.1.3 INTERNATIONAL AND DOMESTIC CORPERATION

In the context of combating hacktivism international and domestic corporations require a unified response. Through ratifications of international conventions, and domesticating provisions of those conventions by State parties, there has been tremendous achievement in the fight against hacktivism. As outlined earlier, the fight against hacktivism and cyber-related crimes is no longer a regional issue.

Council of Europe's Budapest Convention on Cybercrime has broken the barriers by allowing non-EU members to be part of the regional convention to ensure that the fight against cybercrimes goes beyond the European Union jurisdiction**.** The recent UN Convention on cyber-crime ratifies by all UN member Sates further bridges the gap between member states who were not part of the regional treaties to align to international standards consequently enhancing domestic and international cooperation.

[53]Rule 8 International Committee of the Red Cross, 'Eight rules for "civilian hackers" during war, and four obligations for states to restrain them' (Humanitarian Law & Policy Blog, 4 October 2023) https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/ accessed 20 June 2025

3.2 COMBATING HACKTIVISM WITHIN INTERNATIONAL LAW

The legal framework requires that in Combating hacktivism within the context of international humanitarian law concerted efforts from all stakeholders must be applied. States as primary actors in IHL need to adhere to international humanitarian law principles under State responsibility to combat hacktivism.

3.2.1 STATE RESPONSIBILITY

State responsibility in International Humanitarian Law (IHL) holds a state accountable for violations of IHL, requiring it to cease unlawful conduct, provide guarantees of non-repetition, and make full reparations for harm caused[54]. According to the international customary law rule 146, A State is responsible for violations of international humanitarian law attributable to it, including.

(c) violations committed by persons or groups acting in fact on its instructions, or under its direction or control; and

(d) violations committed by private persons or groups which it acknowledges and adopts as its own conduct.

The principle of State responsibility applies to both conventional international warfare and international cyber-crimes. It is trite law that if Hacktivists within a particular State conduct attacks on another State under either an express or implied instruction of that State, that State bears full responsibility under IHL.

States have an obligation under the principle of due diligence not to knowingly allow their territories or cyber infrastructure to be used for acts that affect the rights of other States and cause serious consequences. The principle makes a State responsible for taking all necessary steps to stop hacktivists from conducting crimes from its territories and targeting other states.

The principle of non-intervention is deeply rooted in the concept of state sovereignty, which holds that each state has the right to govern itself without external coercion. Under this principle, international law prohibits states from interfering in the internal affairs of

[54] Sassòli, Marco, 'State responsibility for violations of international humanitarian law' (2002) 84 International Review of the Red Cross pg 404

other sovereign states. Hacktivist operations that are controlled by a state and interfere with a target state's sovereignty maybe be considered a breach of the principle of non-intervention and a violation of sovereignty. This would make the sponsoring state internationally responsible.

The other principle under State Responsibility is Attribution. For a state to be fixed with responsibility, not only must there be an unlawful act or omission, but that unlawful act or omission must be attributable to the State[55]. A key challenge to the principle of attribution is proving that a state is responsible for the acts of a hacktivist group. This is crucial for invoking state responsibility. Attribution may occur if the hacktivists act under the instruction, direction, or control of the state.

3.3 ZAMBIA'S LEGAL FRAMEWORK

Zambia's legal framework in combating hacktivism and other cyber threats can be found in the enactment of its recent revised cyber laws.

3.3.1 LEGISLATIVE ADVANCEMENT

The most recent significant legislative development is a two-part framework that gave rise to **The Cyber Security Act (CSA) of 2025[56]** and **The Cyber Crimes Act (CCA) of 2025[57]** having repealed the former legislation. The Cyber Security Act (CSA) of 2025 establishes Zambia Cyber Security Agency whose functions include among others, take measures in response to cyber security incidents which may threaten critical information, critical information infrastructure or any information or infrastructure in the Republic likely to be affected by a cyber security incident, identify and ensure the protection of critical information and critical information infrastructure and provide technical assistance and collaborate with other relevant national and international institutions in matters relating to this Act[58]. The Cyber Crimes Act of 2025 provides for offences relating to computers and

[55] Dixon, Martín. Textbook on International Law (7th ed) Oxford University Press, USA 2013, pg. 258
[56] Act No 3 of 2025
[57] Act No 4 of 2025
[58] Act No 3 of 2025, Section 4

computer systems, protection of persons against cybercrime provides for child online protection; and provide for matters connected with, or incidental to, the foregoing. Although the term "hacktivism" itself is not expressly used, its primary tactics are criminalized under the Cyber-crimes Act. By applying methods of attack used by Hacktivists, the act by implication targets crimes committed by Hacktivists. Section 3(1) of the cyber-crimes act provides for the Prohibition of unauthorised access to computer system and data which forms an essential element of nearly all hacktivist attacks.

This framework criminalizes the key activities associated with hacktivism. The act further in Section 5[59] criminalises unauthorized disclosure of data, especially relating to critical information or critical information infrastructure which covers hacktivist actions like data theft and information leaks. Section 2 of the act defines “cyber terrorism” to mean the use of a computer or computer system to attack or threaten to attack computers, networks and information stored on the computers and networks with intent to intimidate or coerce a government or its people in furtherance of political or social objectives and to cause severe disruption or widespread fear in society.[60] In terms of cyber terrorism, the Act expressly prohibits cyber-attacks and cyber terrorism, which can encompass large-scale or high-impact hacktivist operations targeting essential services or critical infrastructure.

3.3.2 ALIGNMENT WITH INTERNATIONAL STANDARDS

Zambia is a member of few international conventions that include the recently formed United Nations Convention against Cybercrime and the African Union Convention on Cyber Security and Personal Data Protection. By establishing the Zambia Cyber Security Agency, it reaffirms commitment to Article 27 of the African Union Convention on Cyber Security and Personal Data Protection requirement requiring that State parties to adopt the necessary measures to establish an appropriate institutional mechanism responsible for cyber security governance.

Article 10 of the United Nations Convention against Cybercrime and Section 5 of the Cyber

[58] Dixon, Martín. Textbook on International Law (7th ed) Oxford University Press, USA 2013 Pg257

[59] Act No 4 of 2025, Section 2

[60] ibid

Crimes Act is one of the typical examples of how Zambia's domestic legislation aligns with international standards in combating hacktivism related crimes.

3.4 CONCLUSION

This Chapter highlights how effectively countering the dual threats of hacktivism and cyber warfare necessitates complementary legal and technical architecture that blends the traditional principles of International Humanitarian Law (IHL) with robust cybersecurity frameworks. While IHL provides the necessary ethical and legal boundaries for cyber operations during armed conflict, with adherence to distinction, proportionality, and precaution, technical standards like ISO/IEC 27001 and the NIST CSF establish the preventative measures, incident response protocols, and risk management essential for defense in peacetime and conflict.

The Chapter further underscores that State responsibility is a crucial mechanism for accountability, applying state-sponsored hacktivism and requiring states to exercise due diligence in preventing their cyber infrastructure from being used for attacks on others sovereign states. Furthermore, the push toward international cooperation is evident through multilateral instruments like the global UN Convention against Cybercrime and regional agreements such as the Budapest and Malabo Conventions, which are vital for harmonizing domestic laws and facilitating cross-border enforcement.

Ultimately, Zambia's recent legislative advancements, namely the Cyber Security Act of 2025 and the Cyber Crimes Act of 2025 demonstrate a commitment to this unified approach. By criminalizing key hacktivist tactics and establishing a national cyber security agency, Zambia is aligning its domestic legal framework with international standards, contributing to the collective global effort to minimize the effects of cyber threats and ensure compliance with International Humanitarian Law.

CHAPTER FOUR

CHALLENGES OF APPLYING INTERNATIONAL HUMANITARIAN LAW TO COUNTERACT HACKTIVISM THREATS

4.0 INTRODUCTION

Until recently International Humanitarian Law had fewer challenges in applying its core objectives. However, with technological advancement, methods of warfare in armed conflicts are applied using high tech computer technology that now poses greater challenges in achieving the core principles of international humanitarian Law. This chapter first outlines conceptual and definitional challenges, attribution and identification difficulties. Further the chapter will delve into enforcement and accountability mechanisms, principles of IHL in the technological domain and finally domestic challenges. The Chapter will undertake a case study of **Killnet** their history, motivation, cyber-attacks and States and international organizations' response to cyber-attacks under international Humanitarian Law. Ultimately conclusion of the chapter will be drawn from the foregoing.

4.1 CONCEPTUAL AND DIFINITIONAL CHALLENGES IN INTERNATIONAL HUMANITARIAN LAW APPLICATION

In international humanitarian law (IHL), States, entities and individuals maybe be held liable for violations as subjects of IHL and objects such as specific weapons maybe be prohibited[61]. Rule 149 of the ICRC[62] on Responsibility for violations of International Humanitarian Law specifies subjects that may be held liable to include, States, military personnel, and even private companies and their personnel for direct involvement in IHL violations. The application of IHL to traditional armed conflicts is clear regarding subjects and objects of international humanitarian law, sadly there are inherent challenges in inserting hacktivism into International Humanitarian Law (IHL) framework**.**

[61] https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/what_is_ihl.pdf. Accessed 14 October 2025

[62] https://ihl-databases.icrc.org/en/customary-ihl/v1/rule149. Accessed 14 October 2025

The first challenge is attributed to defining "Hacktivism" under international humanitarian Law and distinguishing "hacktivism" from cyber-warfare, espionage, or criminal activity and whether it can constitute an "armed conflict" or "hostilities" in terms of IHL. Under conventional rules of IHL, principles of distinction and proportionality hinges on whether an armed conflict constitutes an "attack" and such an attack should be one that results in serious injury or death to persons and or damage or destruction to objects. In most cases, hacktivists methods infrequently meet the threshold of an attack thus creating a significant regulatory loophole.

The other challenge is classifying hacktivist as combatants or non-combatants under international humanitarian law which is crucial in dealing with those affected by and those directly participating in an armed conflict. In international humanitarian law, civilians are protected unless they participate directly in an armed conflict, however, there is no clear definition of "Direct participation in hostilities" in cyber related activities. Based on such uncertainty, hacktivists remain classified as civilians and retain immunity from being the object of an attack unless and for such time as they "directly participate in hostilities".

4.2 ATTRIBUTION AND IDENTIFICATION DIFFICULTIES IN THE FIGHT AGAINST HACKTIVISM

Attribution in international humanitarian law (IHL) is the process of determining whether a state is responsible for the conduct of individuals or groups for IHL violations. This is vital for establishing state responsibility for violations of International Humanitarian Law and eventually holds that state accountable. Every internationally wrongful act of a State entails the international responsibility of that State. According to **Article 1** on Responsibility of States for Internationally Wrongful Acts 2001, "Every internationally wrongful act of a State entails the international responsibility of that State."[63]
According to **Rule 15** of the Tallin manual[64], "Cyber operations conducted by organs of a

[63] The International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts (2001). https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf. Accessed on 16 October 2025

[64] Tallin Manual

State, or by persons or entities empowered by domestic law to exercise elements of government authority, are attributable to the State". Attribution arises from several circumstances, however, the clearest is when State organs, such as the military or intelligence agencies, commit wrongful acts. Conversely, it is very difficult to attribute a state to a wrongful act committed by individuals or groups or entities. In such circumstance cyber crimes committed by individuals or groups or entities maybe be equated with State organs even if that status does not follow from internal law, provided that such individuals, groups or entities act in "complete dependence" on the State.
Due to this strict requirement, it is very difficult to attribute a state to cyber acts by hacktivists who are classified as individual or groups and act in 'complete independence' from home States.

4.2.1 ANONYMITY AND PSEUDO-ANONYMITY OF HACKTIVISTS

The conduct of a person or entity which is not an organ of the State but is empowered by law of that state to exercise some government elements will be considered an act of that state[65]. Drawing from this principle of attribution it is therefore imperative under international humanitarian law that perpetrators of violations would easily be identified under traditional warfare. However, the practical obstacles in identifying who is responsible for a hacktivist action, which is essential for IHL compliance and enforcement, possess a huge challenge. Fundamentally, Hacktivists use ultra-modern tools and methods to disguise or fake their identity and remain anonymous, making attribution of cyber operations extremely difficult. Further, Hacktivists' cyber threats often emanate from multiple jurisdictions, stifling investigations, evidence gathering, and the subsequent legal response.

[65] Ibid Article 5

4.2.1 STATE SPONSORSHIP AND PROXY ACTORS

According to Responsibility of States for Internationally Wrongful Acts 2001[66]," The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.

To determine whether a hacktivist group is acting on behalf of or under the **"effective control"** of a state and consequently hold that state responsible for those actions an effective control test extracted from the International Court of Justice's (ICJ) *Nicaragua*[67] case, sets a high standard for attributing the conduct of a non-State actor to a State. To satisfy the test, it must be proved that the State directed or controlled the hacktivist's specific operation, meaning the State exercised complete control over the group and issued specific instructions for each operation.

The other adopted test in IHL is the "**overall control test**" developed by the ICTY as a response to a perceived weakness in the "effective control" test for organized groups, providing a lower evidentiary bar for the prosecution. A State exercises "overall control" over an armed group if it is involved in equipping, financing, and coordinating or planning the group's general military activities. For hacktivist groups, proving that a State controlled the beginning, conduct, and end of a specific cyberattack is nearly impossible. Hacktivists often operate in loose, decentralized structures with political or ideological, not financial, motive, making direct instruction from a State a rare occurrence or at least nearly impossible to prove. Both tests fall short due to the complexity of applying attribution of the state to hacktivists' actions.

4.3 ENFORCEMENT AND ACCOUNTABILITY MECHANISM FOR APPLYING IHL TO HACKTIVISM

The challenge of ensuring compliance and administering consequences for hacktivism violations is complex, primarily due to the distinctive characteristics of cybercrime, the

[66] Ibid Article 8
[67] [1986] ICJ Pg 14

anonymous nature of hacktivist groups, and the lack of a unified international legal framework which may be expanded on the following key issues.

4.3.1. JURISDICTIONAL AND INTERNATIONAL LEGAL HURDLES

Hacktivism is a transnational phenomenon, which imminently complicates the legal process. In some instances, in cross-border jurisdictional issues, a hacktivist attack may involve a perpetrator in one State, affect a victim in a second State, and servers located in a third state. Such complexities call into question about which State has the authority to investigate and prosecute the crime. The **Bangladesh Bank Heist**[68] in 2016 remains one of the most illustrative examples of a complex, cross-border financial cyberattack. Hackers infiltrated the Bangladesh central bank's systems and sent fraudulent SWIFT messages instructing the Federal Reserve Bank of New York to transfer nearly $1 billion. Although most transfers were blocked, $81 million was successfully withdrawn and laundered through Philippine casinos and Sri Lankan banks.
The attack demonstrated not only technological sophistication but also a calculated exploitation of legal and procedural weaknesses.

Another central issue is that of dual criminality. Legal frameworks and definitions of cybercrime vary significantly between nations. Enforcement of cybercrimes relies on international cooperation, which is impeded when crime committed in one state is not considered a crime in another state where the perpetrator is located. Amarachi F. Ndubuisi in his article[69], stated that, “despite the international impact of these crimes, the capacity to prosecute cybercriminals remains deeply rooted in national jurisdictions. Law enforcement agencies face numerous legal and procedural obstacles when attempting to investigate actors beyond their territorial reach. Most notably, the principle of territorial Jurisdiction (a bedrock of criminal law) clashes with the borderless nature of cybercrime.

[68] Corn Geoffrey S, Jensen Eric Talbot. Transnational criminal jurisdiction and extraterritorial enforcement challenges. (*Vand J Transnatl Law)*. 2018;51(4):867–885
[69] Amarachi F. Ndubuisi, CROSS-BORDER JURISDICTION CHALLENGES IN PROSECUTING CYBERCRIME SYNDICATES TARGETING NATIONAL FINANCIAL AND ELECTORAL SYSTEMS (International Journal of Engineering Technology Research & Management, 2022) Vol-06 (Issue 11), 243

These challenges unfortunately tend to exist even in nations with very robust legal frameworks and advanced capabilities.

4.3.2 LACK OF POLITICAL WILL AND EXTRADICTION DILEMMAS

In many cases hacktivism is politically motivated, and a lack of political will from the perpetrator's host State to cooperate with foreign law enforcement agencies leads to serious obstacles. Political and diplomatic corporations usually outweigh bilateral and multilateral agreements and such nations' failure to cooperate with other nations in extradition request impedes the fight to cyber-crimes. Cybercriminals frequently operate from jurisdictions unwilling to surrender suspects, either to protect national security interests or to leverage the suspect for geopolitical negotiation.[70] China and Russia cited as having routinely rejected extradition requests from Western nations, citing sovereignty breach, lack of dual criminality and unwarranted prosecutions. Moreover , both countries have no formal extradition treaties with the USA.

4.3.3 DIGITAL EVIDENCE AND TECHNOLOGICAL GAPS

The ephemeral nature of digital data and the technological disparity between hackers and law enforcement also create significant problems for administering consequences. The following are perceived as the crucial ingredient of the technological gaps

Volatility of Digital Evidence:

It has been observed that digital evidence can easily be altered, destroyed or inadmissible in court if not meticulously maintained during collection and preservation.

Technological Race:

Hackers and hacktivist groups are highly advanced and sophisticated individuals continually evolving their tactics and tools, often staying ahead of law enforcement's investigative techniques and forensic capabilities.

Lack of Expertise and Resources:

Many law enforcement agencies, especially in developing countries, lack the specialized

[70] Ibid 247

technical expertise, trained personnel, and sophisticated forensic labs required to investigate and prosecute complex cybercrimes.

4.3 DOMESTIC CHALLENGES IN APPLYING INTERNATIONAL HUMANITARIAN LAW

Applying International Humanitarian Law (IHL) to counteract hacktivism threats presents significant challenges for any state, including Zambia, primarily because IHL is designed for situations of armed conflict, which hacktivism rarely meets. Domestically, these challenges are compounded by legal and practical gaps.

4.3.1 ZAMBIA'S NEW DOMESTIC CYBER FRAMEWORK

Zambia's new domestic cyber framework is two folds, the Cyber Security Act, 2025 (CSA)[71] provide for cyber security in the Republic, establishes the Zambia Cyber Security Agency and provide for its functions. The Cyber Crimes Act, 2025 (CCA)[72] provides for offences relating to computers and computer systems and protection of individuals against cybercrimes. Despite major breakthroughs made by the new pieces of legislation in terms of Prohibition of Cyber Attack, Cyber Terrorism and Protection of Critical Information Infrastructure[73], there are many challenges faced in applying the laws regarding hacktivism. For instance, effectiveness of the two pieces of legislation is hindered by omission of key terms like 'hack back', 'hacktivism' or 'hacktivist'[74] and how cyber attacks such as Dedicated denial of service can be mitigated in line with IHL. Further, challenges are outlined below.

4.3.1 TECHNOLOGICAL DISPARITY

In most cases, hacktivists are highly skilled and use very sophisticated tools which makes law enforcement agencies unable to find these perpetrators. Moreover, Zambia's law

[71] Act No 3 of 2025
[72] Act No 4 of 2025
[73] Ibid, section 2
[74] Tallin's Manual

enforcement agencies have limitations in both skills and tools to handle cybercrimes. This may be attributed to lack of adequate funding to these institutions.

4.3.2 JUDICIAL EXPERTISE

The judiciary and law enforcement may not be adequately trained to handle cases involving complex cyber-attack attribution or to interpret the interplay between the new Cyber Laws, the Penal Code, and underlying IHL principles. The cyber crimes Act and Cyber security act, though recently enacted, do not fully provide comprehensive legal backing to counteract hacktivism. This is due to the rapid nature of technological advancement.

4.3.3 CAPACITY AND ATTRIBUTION LIMITATIONS

Capacity and attribution limitations may be drawn from the lack of the specialized technical capacity to effectively attribute a cyber-attack to a specific hacktivist group and determine if the attack has crossed the threshold into an IHL. This may include the lack of tools that can be used to determine the type of attack and the impact on critical civilian infrastructure.

4.2 A CASE STUDY OF KILLNET

Killnet is a pro-Russian hacktivist group that emerged shortly after the start of the Russian – Ukraine war in 2022.

4.4.1 MOTIVATION

The group's actions are driven by **pro-Russia** sentiment, targeting nations and organizations that support Ukraine or oppose the Kremlin's policies[75]. Killnet mainly applies DDoS (Distributed Denial of Service) attacks to disrupt service of its targets.

[75] Cyber Intelligence Bureau Orange Cyberdefense https://www.orangecyberdefense.com/fileadmin/global/CyberIntelligenceBureau/Gangs_Investigations/KillNet/KillNet-PMHC-KillNet-Black-Skills-Entities.pdf. Accessed 18 October 2025

Their motivation is worldly considered to be politically aligned to defend Russian interests, targeting countries and organizations directly supporting Ukraine or opposing Kremlin policies.

4.4.2 MAJOR CYBER-ATTACKS AND TARGETS ATTRIBUTED TO KILLNET

The group mainly targets government, financial, health, and media sectors in Western countries and NATO allies. In May 2022, “Pro-Russian hackers have attacked the websites of several Italian institutions, including the senate, ANSA news agency reported on Wednesday. The hacker group "Killnet" claimed the attack, ANSA said, which also targeted the National Health Institute (ISS) and the Automobile Club d'Italia, a national drivers' association” Reuters news[76].

In August 2022, Lockheed Martin was targeted with a distributed denial of service attack delivered by pro-Russian hacker group Killnet. The information came via the Moscow Times who reported Killnet claimed responsibility.[77]

In June 2022, Russian hacker group Killnet claimed responsibility for a denial-of-service (DDOS) cyberattack on Lithuania, saying it was in response to the decision by Vilnius to block the transit of some sanctioned goods to the Russian exclave of Kaliningrad” Aljazeera News[78]. In all these attacks, the motivation is tied to the principle that the hacktivist group, were satisfying their support to Russia and against those states in support of Ukraine.

4.3.4 STATES AND INTERNATIONAL ORGANISATION’S RESPONSE TO KILLNET ATTACKS

States and international organisation’s response to Killnet's attacks under International Humanitarian Law (IHL) has been complex. The main reason is that Killnet is a non-state

[76] https://www.reuters.com/world/europe/pro-russian-hackers-target-italy-defence-ministry-senate-websites-ansa-news-2022-05-11. Accessed 20 October 2025

[77] https://www.securityweek.com/killnet-releases-proof-its-attack-against-lockheed-martin/. Accessed 20 October 2025

[78] https://www.aljazeera.com/news/2022/6/27/russia-hackers-claim-responsibility-for-cyber-attack-on-lithuania accessed 20 October 2025

hacktivist group and most of their attacks (DDoS) typically fall below the high threshold of an "armed attack" or "use of force" that activates a military response under International Humanitarian Law.

International humanitarian Law principles only apply to cyber operations that are conducted during armed conflict. However, most attacked conducted by Killnet such as Denial-of-service attacks despite been disruptive do not meet the criteria of a cyber attack under IHL by the mere fact that, it requires that an attack should cause injury or death to persons or destruction or damage to civilian objects.[79]

To bring perpetrators acting under Killnet criminally liable, States and international organisations must apply the principle of distinction. Killnet attacks on civilian objects like financial institutions, musical concerts, hospital and non-military institutions are contrary to IHL principles of distinction which make perpetrators liable.

International orgainsations like the international committee of red cross (ICRC) has directly appealed to hacktivist groups, including Killnet, to comply with a set of "Rules of Engagement for Hacktivists," which include, refraining from direct cyberattacks against civilian objects like medical and humanitarian facilities and making threats of violence to spread terror among the civilian population.

Since Killnet attacks normally fall below the required military threshold, States's primary response is usually under domestic criminal law.

4.6 CONCLUSION.

In essence, the core difficulty is that cyberspace affords high technical anonymity for decentralized actors operating across borders, which systematically undermines the traditional legal mechanisms built on physical jurisdiction and clear attribution.

The chapter explores the significant challenges states face in applying International Humanitarian Law (IHL) to politically or ideologically motivated hacktivism, arguing that IHL's traditional framework is ill-suited for this contemporary threat**.** The core challenge

[79] Tallinn manual rule 92

is that IHL principles, such as distinction and proportionality, only apply to cyber operations that constitute an "attack. Most hacktivist methods, like Distributed Denial of Service (DDoS) attacks, are disruptive but infrequently meet this high threshold, creating a regulatory loophole.

Establishing State responsibility for hacktivist actions is nearly impossible. Hacktivists operate with anonymity/pseudo-anonymity and typically act in 'complete independence' from their home states.

Enforcement is further complicated by the transnational nature of hacktivism, where perpetrators, victims, and servers often reside in different jurisdictions. Issues like dual criminality and a lack of unified international legal frameworks impede cross-border cooperation. A lack of political will from host states, which may harbor hacktivists for geopolitical leverage (e.g., in China and Russia), creates safe havens and complicates extradition

Domestically, states like Zambia face challenges even with new legislation like the Cyber Security Act, 2025. The effectiveness of these laws is hampered by the omission of key terms like 'hacktivism' and 'hack back,' coupled with technological gaps, capacity limitations, and insufficient judicial expertise to handle complex cyber-attack attribution

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.0 INTRODUCTION

The chapter summarizes the information presented in the dissertation's earlier chapters. It attempts to give a summary of the

5.1 GENERAL CONCLUSIONS

This study sought to assess the legal framework on International Humanitarian Law and examine the core treaties under IHL that relate to hacktivism and cyber warfare. Role of International Humanitarian Law and cybersecurity frameworks in combating hacktivism and cyber warfare. Finally, the challenges of applying International Humanitarian Law to counteract hacktivism threats.

It was observed that, even though the application of IHL in its traditional form has been successful, there are huge challenges in applying IHL principles in modern warfare mainly due to attribution challenges, technological gaps, Lack of political will from host states, Extradition dilemmas, lack of judicial expertise and domestic challenges.

5.2 SUMMARY OF CHAPTERS

The thesis consists of five chapters which assess the effectiveness of international humanitarian law in regulating hacktivism in cyber warfare with specific reference to a case study of Killnet.

5.3 CHAPTER ONE

In the first chapter the legal issue was identified thereby creating a foundation for the

research study. The chapter underscores the three objectives of the study which had been refined in the proceeding chapters. Furthermore, this Chapter also highlighted the significance of the study. In this chapter it was concluded that while IHL principles rooted in military necessity and humanity are universally applicable to all forms of warfare, their effectiveness in regulating cyber conflicts, particularly those involving hacktivism, is severely challenged by issues of ambiguity and application. Although, core principles of IHL remain the essential guide for preserving humanity in cyber conflicts, their practical application requires urgent refinement and clarity to overcome the challenges of anonymity and identification

5.4 CHAPTER TWO

This chapter focused on assessment of the legal framework on International Humanitarian Law and examining the core treaties under IHL that relate to hacktivism and cyber warfare. This chapter revealed that IHL principles generally do apply to cyber warfare when operations cause injury, death, damage, or destruction meeting the definition of an "attack" under IHL. A cyber operation that causes physical effects and harm is treated similarly to a traditional military attack, subjecting the perpetrating State to responsibility for IHL violations.

The principle of proportionality also applies, prohibiting cyber acts that cause adverse suffering disproportionate to the military gain. Further, the chapter outlined that applying IHL to hacktivism is far more complex mainly because IHL hinges on the existence of armed conflict. Therefore, if a hacktivist operation is the sole means of hostile action between states, or if it is conducted by non-state actors (hacktivists) without reaching the threshold of a non-international armed conflict, IHL rules may not apply. Hacktivist actions are unlikely to meet the IHL definition of an "attack" because they often lack the kinetic effect of causing physical harm.

While IHL, guided by principles like military necessity, is meant to apply to "all forms of warfare, including those of the “future," its framework is stretched by non-kinetic cyber threats. Cyber warfare causing physical harm is generally covered, but hacktivism often falls below the required threshold of armed conflict or a destructive attack, challenging the established definitions of combatants, civilians, and attacks within IHL.

5.5 CHAPTER THREE

This chapter assesses the complementary roles of International Humanitarian Law (IHL) and modern cybersecurity frameworks in countering threats posed by hacktivism and cyber warfare, examining how states, including Zambia, integrate these structures into hacktivism and cyber warfare threats while complying with International Humanitarian Law.

International humanitarian law is derived from the Geneva Conventions and Customary International Law, primarily aiming to limit suffering during armed conflict. For IHL to apply to hacktivism or cyber warfare, the operation must meet the high threshold of an armed conflict and adhere to core principles like distinction, proportionality, and precaution, causing significant harm to civilian objects.

The chapter highlighted that until now since a single global cyber treaty was lacking, international cooperation was driven by regional and global conventions. The Council of Europe's Budapest Convention on Cybercrime provides a key framework for criminalizing cybercrimes and enabling cross-border judicial cooperation. The African Union’s Malabo Convention focuses on cybersecurity, data protection, and crime within the continent.

The recently adopted UN Convention against Cybercrime aims to strengthen global cooperation, criminalization, and technical assistance among all member states.

The chapter also outlined the Cybersecurity frameworks provide the proactive, preventative counterpart to IHL's reactive war-time rules:

While IHL limits harm during conflict (e.g., prohibiting attacks on civilian infrastructure), cybersecurity frameworks build defenses and legal accountability to prevent attacks altogether, thus minimizing the potential for IHL violations.

The combined role of IHL principles, international treaties, and robust domestic cybersecurity frameworks is essential for creating a multilayered defense against complex cyber threats.

5.6 CHAPTER FOUR

provides an in-depth analysis of the inherent difficulties in applying International Humanitarian Law (IHL) principles to modern cyber threats, particularly those posed by hacktivism.

The primary challenge is the lack of clear definitions to bridge IHL's traditional rules with the digital domain. Most hacktivist actions do not meet the IHL threshold of an "attack", which requires an action to cause serious injury/death or destruction/damage to objects. This creates a regulatory loophole, as many disruptive cyber methods (like DDoS) fall below this bar. It is unclear how to classify hacktivists (who are non-state actors) under IHL. As they lack a clear definition of **"**Direct participation in hostilities**"** in a cyber context, they are often classified as civilians, retaining immunity from being targeted even while engaged in cyber operations.

Holding states or groups accountable is extremely difficult due to the nature of cyberspace. In most cases Hacktivists use sophisticated tools to conceal their identities and operate across multiple jurisdictions, making attribution nearly impossible.

However, even when an actor is identified, enforcing IHL and prosecuting them faces major obstacles due to Jurisdictional Complexity, Dual Criminality and lack of Political Will and compounded by technological

Domestic challenges and drawn from Zambia, illustrates how domestic laws still struggle to fully address hacktivism. Zambia’s new cyber laws, the Cyber Security Act, 2025 and the Cyber Crimes Act, 2025 are positive steps but fail to define key terms like 'hacktivism' or 'hack back'. This omission, coupled with technological limitations and a lack of judicial expertise to interpret the new laws alongside IHL principles, limits the ability of domestic institutions to effectively mitigate hacktivism threats.

5.7 RECOMMENDATIONS

Having highlighted the legal gaps, challenges, and proposed solutions within the research. The author will proceed and make recommendations with core focus is closing the gap between traditional IHL and the digital reality of cyber conflict and imploring that the global community, states, and non-state actors must take specific actions to ensure International Humanitarian Law (IHL) remains relevant and effective in the face of hacktivism and cyber warfare

5.7.1 CLARIFY AND REINTERPRET CORE INTERNATIONAL PRINCIPLES

The most critical recommendation is to address the ambiguity in applying foundational IHL rules to cyberspace:

States and international bodies must work to establish a clear, shared legal definition of a cyber 'attack' under IHL to determine when an action crosses the threshold of armed conflict and violates the rules of war. Further, there must be a clear legal interpretation of the Principle of Distinction to classify hacktivists and other non-state cyber actors. A clear classification of hacktivists will determine whether they are considered combatants, non-combatants, or organized armed groups, which affects their protection status and accountability.

5.7.2. STRENGTHEN STATE RESPONSIBILITY AND DUE DILIGENCE

To combat state-sponsored or state-enabled hacktivism, the research implicitly recommends strengthening accountability. Countries must strictly adhere to the IHL rule that holds them accountable for violations committed by hacktivist groups acting under their direction, control, or with their implicit acknowledgment.

States must comply with the principle of due diligence by taking all necessary steps to prevent their territories or cyber infrastructure from being used by hacktivists to launch

attacks against other states.

5.7.3. ENHANCE DOMESTIC AND INTERNATIONAL LEGAL COOPERATION

To create a unified defense against transnational cyber threats, cooperation must be mandatory. Key to this, is to promote Global treaty adoption, States, especially non-members of regional frameworks like the Malabo Convention, should ratify and implement global treaties like the UN Convention against Cybercrime to harmonize domestic laws and improve cross-border cooperation in investigations.

Member states must endeavor to domesticate the provisions of international conventions and treaties to ensure that violations of IHL or cybersecurity laws by hacktivists can be prosecuted effectively at the national level.

5.7.4. ADOPTION OF CYBERSECURITY FRAMEWORKS

It is imperative that both state and non-state actors prioritize protection of critical Infrastructure through Identification and Protection functions of frameworks like the NIST CSF to safeguard critical information infrastructure from hacktivist threats, thereby minimizing potential harm to the civilian population. Moreover, organisations may consider implementing robust standards adopted from recognized cybersecurity frameworks like ISO/IEC 27001, NIST CSF 2.0, or CIS Controls.

BIBLIOGRAPHY

STATUTE

The Cyber Crimes Act No 4 of 2025

The Cyber Security Act No 3 of 2025

CASES

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14

INTERNATIONAL LEGAL INSTRUMENT

African Union Convention on Cyber Security and Personal Data Protection, adopted 27 June 2014, entered into force 8 June 2023, African Union

Convention on Cybercrime, ETS No. 185 (23 November 2001).

Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (Geneva, 12 August 1949)

Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention) 1949, 75 UNTS 287

United Nations, United Nations Convention against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, 24 December 2024 (Resolution 79/243)

ISO/IEC 27001:2022, Information technology — Security techniques — Information security management systems — Requirements

ARTICLES

Amarachi F. Ndubuisi, CROSS-BORDER JURISDICTION CHALLENGES IN PROSECUTING CYBERCRIME SYNDICATES TARGETING NATIONAL FINANCIAL AND ELECTORAL SYSTEMS (International Journal of Engineering Technology Research & Management, 2022) Vol-06 (Issue 11)

Corn Geoffrey, Jensen Eric Talbot. Transnational criminal jurisdiction and extraterritorial enforcement challenges. (*Vand J Transnatl Law)*. 2018;51(4)

Crawford, James, Jacqueline Peel, and Simon Olleson. "The ILC's Articles on Responsibility of States for Internationally Wrongful Acts: Completion of the Second Reading." *European Journal of International Law* 12.5 (2001)

Dinstein, Yoram. *The Conduct of Hostilities under the Law of International Armed Conflict*. Cambridge: Cambridge University Press, 2004

Fry, James D. "Attribution of responsibility." Principles of shared responsibility in international law: An appraisal of the state of the art (2014):

International Humanitarian Law Handbook for Parliamentarians N° 25

Responsibility of States for Internationally Wrongful Acts, annexed to GA Res 56/83, UN Doc A/RES/56/83 (12 December 2001)

Sassòli, Marco, 'State responsibility for violations of international humanitarian law' (2002) 84 International Review of the Red Cross

BOOKS

Dixon, Martin, Robert McCorquodale, and Sarah Williams. *Cases and materials on international law* (6th ed) Oxford University Press, USA, 2011.

La Crowe, Jonathan, and Kylie Weston-Scheuber. Principles of International humanitarian Law. Edward Elgar Publishing, 2013

Schmitt, Michael N., ed. *Tallinn manual 2.0 on international law applicable to cyber operations*. Cambridge University Press, 2017.

Dixon, Martin. Textbook on International Law(7th ed) Oxford University Press, USA, 2011

INTERNET SOURCES

International Committee of the Red Cross Database, Customary IHL , Definition of Combatants, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule3 accessed on 17 April 2025)

Applying International Humanitarian Law to Cyber Warfare', Law and National Security: Selected Issues, Containing: Applying International Humanitarian Law to Cyber Warfare https://www.jstor.org/stable/pdf/resrep08957.8.pdf accessed 20 April 2025

https://international-review.icrc.org/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber-913. Accessed on 17 April 2025

https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf accessed 16 April 2025

https://www.xcitium.com/knowledge-base/hacktivism/#:~:text=In%20an%20era%20where%20digital,influence%20in%20today's%20interconnected%20society accessed 15 April 2025

Gawel, H. 'Hacktivism' Internet Policy Review (2004),13(2). https://policyreview.info/glossary/hacktivism (accessed 17 April 2025)

Halme-Tuomisaari, M, 'International Humanitarian Law 'in A De Lauri (ed), Humanitarianism:Keyword (Brill 2020), http://www.jstor.org/stable/10.1163/j.ctv2gjwwnw. Accessed 12 Apr. 2025

International Committee of the Red Cross, 'Eight rules for "civilian hackers" during war, and four obligations for states to restrain them' (Humanitarian Law & Policy Blog, 4 October 2023) https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/ accessed 16 June 2025

International Committee of the Red Cross, *Customary IHL Database*, Rule 149 (14 August 2005) https://ihl-databases.icrc.org/en/customary-ihl/v1/rule149 accessed 14 October 2025

News Agencies, 'Russian hackers claim responsibility for cyberattack on Lithuania' (27 June 2022) *Al Jazeera* https://www.aljazeera.com/news/2022/6/27/russia-hackers-claim-responsibility-for-cyber-attack-on-lithuania accessed 20 October 2025

Orange Cyberdefense Cyber Intelligence Bureau, *PMHC KillNet and Black Skills entities* (Report,2023) https://www.orangecyberdefense.com/fileadmin/global/CyberIntelligenceBureau/Gangs_Investigations/KillNet/KillNet-PMHC-KillNet-Black-Skills-Entities.pdf accessed 18 October 2025

Reuters, 'Pro-Russian hackers target Italy defence ministry, Senate websites: ANSA' (11 May 2022) https://www.reuters.com/world/europe/pro-russian-hackers-target-italy-defence-ministry-senate-websites-ansa-news-2022-05-11 accessed 20 October 2025

The Principle of Distinction: Cyber Operations During Armed Conflict" international committee for the Red Cross. https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf . accessed 20 April 2025

Townsend, K, 'Killnet Releases 'Proof' of Its Attack Against Lockheed Martin' (12 August 2022) *SecurityWeek* https://www.securityweek.com/killnet-releases-proof-its-attack-against-lockheed-martin/ accessed 20 October 2025

https://news.un.org/en/story/2024/12/1158521

Xcitium, 'What is Hacktivism?' https://www.xcitium.com/knowledge-base/hacktivism/ (accessed 17 April 2025)

DISSERTATION AND OBLIGATORY ESSAYS

Samuel, Alexandra Whitney. *Hacktivism and the future of political participation*. Harvard University, 2004

UNIVERSITY of LUSAKA

Passion for Quality Education: Our Driving Force

SCHOOL OF LAW

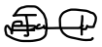
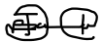
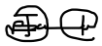
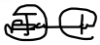
L400B / Dissertation II – DIRECTED RESEARCH (OBLIGATORY ESSAY)

RESEARCH CLEARANCE FORM

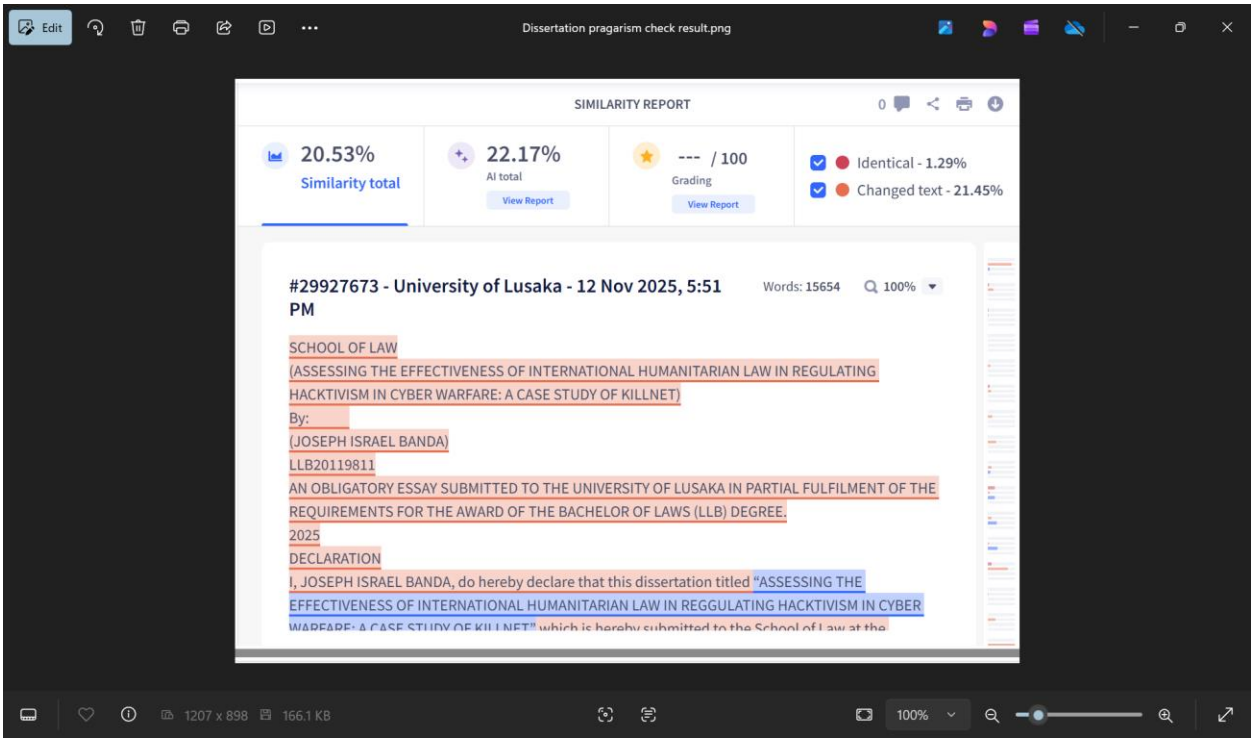
NAME: JOSEPH ISRAEL BANDA **STUDENT NUMBER:** LLB20119811

SUPERVISOR: MR J.M MWACHUKA **TOPIC:** ASSESSING THE EFFECTIVENESS OF INTERNATIONAL HUMANITARIAN LAW IN REGULATING HACKTIVISM IN CYBER WARFARE: A CASE STUDY OF KILLNET

Stage	Supervisor's Comments	Supervisor's Signature & Date	Student's Signature & Date
Research Proposal	APPROVED		1August 2025
Chapter 1 – Introduction	11		5th August 2025
Chapter 2 –	11		12 August 2025
Chapter 3 –	11		14 October 2025
Chapter 4 –	11		22 October 2025

Chapter 5 – Conclusions & Recommendations	"		 24 October 2025
Abstract, Table of Contents, Bibliography and Appendices	"		 26 October 2025
First Draft	"		 29 October 2025
Second Draft	"		 6 Nov 2025
Final Draft	"		 12 Nov 2025

Please attach this form to the back of your dissertation at the end of the research, before submission via the Moodle e-learning platform.


Edit
Dissertation pragarism check result.png
SIMILARITY REPORT
0
20.53%
Similarity total
22.17%
AI total
View Report
--- / 100
Grading
View Report
Identical - 1.29%
Changed text - 21.45%
#29927673 - University of Lusaka - 12 Nov 2025, 5:51 PM
Words: 15654
100%
SCHOOL OF LAW
(ASSESSING THE EFFECTIVENESS OF INTERNATIONAL HUMANITARIAN LAW IN REGULATING HACKTIVISM IN CYBER WARFARE: A CASE STUDY OF KILLNET)
By:
(JOSEPH ISRAEL BANDA)
LLB20119811
AN OBLIGATORY ESSAY SUBMITTED TO THE UNIVERSITY OF LUSAKA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE BACHELOR OF LAWS (LLB) DEGREE.
2025
DECLARATION
I, JOSEPH ISRAEL BANDA, do hereby declare that this dissertation titled "ASSESSING THE EFFECTIVENESS OF INTERNATIONAL HUMANITARIAN LAW IN REGGULATING HACKTIVISM IN CYBER WARFARE: A CASE STUDY OF KILLNET" which is hereby submitted to the School of Law at the
1207 x 898
166.1 KB
100%