Journal of Contemporary African Legal Studies: **Volume 1, Issue 2, 2023, pp. 89-106**

ISSN 2820-2619 ONLINE
ISSN 2820-2627 PRINTED

PROTECTION OF HUMAN DIGNITY IN THE CONTEXT OF CYBER WARFARE: THE STATUS QUO OF INTERNATIONAL LAW REGULATING THE USE OF FORCE

Hellen Luchagula[*]

Seraphina Bakta[**]

ABSTRACT

The protection of human dignity is fundamental basis for the development of human rights and humanitarian law. Currently, cyber operations in warfare are becoming a humanitarian concern because of their ability to incapacitate infrastructure and affect the provision of essential services to civilians. The use of force under the international legal regime is still the same as it had been prior to these developments. Considering its effects on human dignity, the extent to which the conventional methods and the legal framework are adequate to counter such use becomes relevant. This article examines the adequacy of international law on the use of force in protecting human dignity in cyber warfare. The article is based partly on the empirical study, 'Regulating the use of force in international law: An appraisal of the conventional methods in regulating cyber warfare' by the authors. It employs both empirical and documentary review methods to address this matter. It is argued in this article that the existing regime is not sufficient because it is too obsolete. Furthermore, because of the unique features of cyberspace, the regime does not adequately ensure the respect for human dignity.

Keywords*: Cyberspace, Cyber warfare, Human dignity, International law, Use of force.*

[*] Author holds an LL.M from Mzumbe University in Tanzania.
[**] Author is a senior lecturer in law at Mzumbe University in Tanzania.

The use of ICTs in future conflicts between states is becoming more likely. We share this concern and we should add that the use of ICTs in armed conflicts has in fact been a reality for several years, posing a real risk of harm to civilians, civilian infrastructure and societies. In light of this realty, we cannot over-emphasise the need for dedicated discussions on topics of international law: -Ambassador Gafoor, July 2022.[1]

1.0 INTRODUCTION

War has been a catastrophic phenomenon for humanity since the dawn of civilization. It is closely linked with technological developments that have converted scientific fiction to reality in the arena of warfare. Technology is changing every aspect of human life and is, unfortunately, opening prospects of serious danger to the future with more unpredictability, uncertainties, and insecurities. The use of force in cyberspace is capable of shutting down power grids. It means that, all systems requiring electricity supply may not be able to operate; civilians can be deprived of necessities; the supply of water, financial and health services can be affected (since most health care systems are digitalized).[2] Cyber attacks in war can also interfere with rescue services that seek to save lives.[3] As a result, the well-being of thousands of people may be jeopardized and the respect for human dignity be impacted. In the light of the fact that the methods applied in cyber warfare are new and unique,[4] the sufficiency and efficacy of international law on the use of force in guaranteeing the protection of human dignity has been challenged. The issue is that, so far, there is no formal, legally binding agreement on how to apply international law concepts to cyber warfare. It seems, therefore, that traditional methods of regulating warfare are being overridden by cyber warfare methods. The situation poses a serious challenge on international law regulating warfare.

Because the key purpose of international law on the use of force is to protect human dignity by protecting civilians from atrocities, this article, which is divided into six sections, aims at examining the sufficiency of the international legal regime in ensuring respect for human dignity in cyber warfare.

---

[1] International Committee of the Red Cross (ICRC), Statement made by the International Committee of the Red Cross (ICRC) on International Law at the Third Meeting of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 <https://www.icrc.org/en/document/icts-armed-conflicts-risk-harm-civilians-civilian-infrastructure?amp> accessed 21\September 2022.

[2] BBC News, [11 January, 2017], 'Ukraine Power Cut Was Cyber-attack'<https://www.bbc.com/news/technology-38573074.amp> accessed 17 October 2022.

[3] Ibid.

[4] Martin C Libicki *Conquest in Cyberspace* (Cambridge University Press 2007), 26.

After this introduction, section two describes the methodology used; section three provides a background to the topic; section four highlights some distinctive features of cyber war. Section five answers the question why international law on the use of force is insufficient to protect human dignity in cyber warfare; and section six presents the article conclusions.

2.0 METHODOLOGY

This study employed documentary review and interviews methods in collecting data. Documentary review employed both primary and secondary sources.[5] These include international legal materials such as treaties, charters, declarations, and resolutions, while in the context of domestic law secondary sources including, books, journal articles and reports. The international law (primary source) informed the study on the existing international legal framework and, particularly, the evaluation of the adequacy of the regime in regulating warfare. Besides, the international and domestic secondary sources were relevant in understanding the current debate on the adequacy of the law on the use of force in cyber warfare. It needs to be noted that the use of force in general and cyber warfare in particular are regulated by international law. Thus, the analysis of the extent to which the international legal framework affords the protection of human dignity relied on its evaluation as a primary source of data. The study employed both in-person and virtual interviews to collect empirical data. A total number of 25 respondents were interviewed, these being 12 international law practitioners and experts in the area of international law, specifically in international humanitarian law and cyber law; 10 respondent experts in cyber technology; and three military personnel. The interviews provided insights on how to deal with the subject matter from a practical point of view. Additionally, the interviews provided a validation of the data obtained through the documentary review.

3.0 SETTING THE SCENE - CYBER WARFARE AND HUMAN DIGNITY

As a humanitarian concept, human dignity is the entitlement of all human beings to be treated with esteem and respect merely for possessing human attributes.[6] It is the sense of worthiness and value that accompanies every human being. This rule establishes the foundation upon which human beings can live in harmony, fend off mistreatment, and withstand the prospect

[5] It has to be noted that in the legal context legal instruments both at international law constitute a primary source of data, while other materials such as reports, books and journal articles are regarded as secondary sources.

[6] Gan Shaoping & Zhang Lin, 'Human Dignity as a Right' (2009) 4(3), 370 Frontiers of Philosophy in China, 370.< http://www.jstor.org/stable/40343932> accessed 28 of September 2021.

of self-destruction.[7] Thus it is the foundational rationale for all measures taken to safeguard and sustain human well-being. Considering that human life is inviolable, the sanctity of life is the basic value that underpins the right to dignity. Human dignity is violated where human life is threatened. Such actions may injure the victim's physical, psychological, social or economic state or impair their ability to protect themselves or to anticipate external protection.[8]

All human beings deserve to be treated respectfully in all circumstances, regardless of their status.[9] War by its very nature debases the human dignity of those, particularly innocent civilians, caught in the crossfire. This is because war is characterized by actions or omissions that have detrimental impacts on the fundamental ability of humans to live a self-directed life within the confines of desirable living standards and morality. Just like human rights, in warfare the protection of human dignity is only guaranteed for those groups of protected persons and property under international humanitarian law.[10]

It has been noted that the deployment of scientific and technological progressions, cyber warfare included, are capable of undermining the respect for human dignity.[11] Cyber warfare entails all means and methods of war employed in cyberspace intending to undermine the functioning capacity of a computer system.[12] The reason can either be military, political, economic, or financial or for securing national security.[13] Considering that currently many aspects of human life are linked to computer systems, the welfare and dignity of innocent civilians may be directly affected in a cyber war.

[7] ibid.
[8] ibid.
[9] United Nations, Preamble to the Charter of the United Nations [24 October 1945] 1 UNTS XVI [hereafter referred to as the UN Charter]; art 1 of the Universal Declaration of Human Rights; Article 10 of the International Covenant on Civil and Political Rights of 1966; and art 13 of the International Covenant on Economic and Social Cultural Rights of 1966.
[10] Protected persons under IHL include religious, medical, and humanitarian personnel, civilians and *hors de combat*. See arts13, 24, 25, 26, 38 and 44 of the First Geneva Convention; arts 13, 36, 37, 41 and 43 of the Second Geneva Convention ;arts 4 and 6 of the third Geneva Convention, arts 4 and 20 of Geneva Convention IV;art 38 of the Additional Protocol I; and art 12 of Additional Protocol II.
[11] The UN Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind of 1975.
[12] Khatuna Burkadze, 'A Shift in the Historical Understanding of Armed Attack and Its Applicability to Cyberspace' (2020) 44 (1) The Fletcher Forum of World Affairs 33<https://www.jstor.org/stable/10.2307/48599279> accessed 31 June 2022.
[13] Oona A Hathaway and others, 'The Law of Cyber-Attack' (2012) 100 (4) California Law Review, 817<,https://www.jstor.org/stable/23249823> accessed 19 December 2021.

Even though cyber attacks have not caused such serious physical repercussions so far, the world should be warned about the humanitarian concerns that may arise out of it.[14] Consider an instance where a nuclear power plant is made to erupt or cyber attacks target dams which protect densely populated countries from flooding. Consider, too, the failure of computer systems to operate in hospitals and as a result diagnostic devices cannot function, or where civilians cannot access safe and clean water and banking systems cannot operate. Consider, also, if communication, transport and traffic systems in busy cities are infiltrated, resulting in accidents, traffic jams and communication lines being shut down. Consider, further, if billions of people fall off the grid, and people are trapped in elevators and subways in big cities. Finally, consider the impact of a computer virus causing a malfunction in a nuclear reactor. All these may cause panic among civilians, affect living conditions, and cause physical and psychological torture, devastation and even death. Such massive attacks may result in a humanitarian catastrophe and directly affect innocent civilians. In this respect, human dignity is likely to be undermined in a cyber war.

4.0 UNDERSTANDING CYBER WAR: SOME DISTINCTIVE FEATURES

The following features are unique to a cyber war. It is because of these unique features that the law on the use of force and war should be examined to confirm its efficiency in affording respect for human dignity in cyber warfare.

4.1 Cyberspace as a war domain

Etymologically, the word cyberspace is a combination of two words; cyber (netics) + space = Cyberspace.[15] The word cyber owes its origin to ancient Greek word *Kubernetes,* which means, the one who governs.[16] The compound word cyberspace first appeared in the 1982 short story '*Burning Chrome'* and, later, in 1984, in the scientific narrative *Neuromancer* by William Gibson.[17] The word was used to mean anything that is related to the Internet. In the opinion of the International Telecommunications Union of the United Nations (ITU), the realm of cyberspace comprises computers, computer systems, networks, and associated

[14] Stephan Koloßa 'Is There Really a Need for a New "Digital Geneva Convention"?' (2019) 2 (1/2) Völkerrecht Humanitäres: Journal of International Law of Peace and Armed Conflict,. 37.<https://www.jstor.org/stable/48540658> 29 July 2022.
[15] The Vocabularist (15 March, 2016). 'How We Use the Word Cyber '< https://www.bbc.com/news/magazine-35765276> accessed 20 March 2022.
[16] ibid.
[17] William Gibson, *Neuromancer* (2009 Ace), 4–5, 38, 43.

software, data and users,[18] as well computer networks dealing with the creation, sharing and storage of data or information. As a domain of war, cyberspace is comprised of three elements: People, tools and weapons.[19] People use computer tools to develop programs that are cyber weapons.

Unlike in conventional fields, in cyberspace a difference in geographical positions is not an impediment. Rather, the determination of proximity between the adversaries is dependent upon bandwidth and connectivity.[20] Nevertheless, the field lacks boundaries; the effects of an attack launched against state A may affect civilians in state B and even in other states. Even though cyberspace is qualitatively distinct from other domains of warfare, it overlaps and operates within all other domains,[21] allowing it to be used as an adjunct to conventional warfare. According to the United States' Presidential Policy Directive (PPD-21),[22] in a cyberwar, the cyberspace of critical infrastructure is targeted. So far, 16 infrastructures have been identified as being susceptible and vulnerable targets in a cyber war.[23] These infrastructures are directly linked to the well-being of civilians.

The core challenge in addressing violations of human dignity in cyber warfare is the nature of the cyber field which is generally described as an abstract domain. It is a field imperceptible to the naked eye and it does not need bombs or guns to execute a military mission. It is cheap, easy, and allows an attack to be executed within microseconds as compared to conventional warfare.[24] Because cyberspace guarantees interconnectivity, cyber warfare is a matter of concern not only to technologically advanced nations, but to all nations. A single intentional

[18] ITU *Toolkit for Cybercrime Legislation*, 12< ww.itu.int/cybersecurity> accessed 19 December 2021.
[19] John B Sheldon, 'Cyberwar' in *Encyclopaedia Britannica* (2023) <, https://www.britannica.com/topic/cyberwar> accessed 17t March 2022.
[20] M Gomez 'Cyber Enabled Information Warfare and Influence Operations' in C Whyte, and others (eds), *Information Warfare in the Age of Cyber Conflict* (Routledge 2021), 38.
[21] Fred Schreier 'Cyberwarfare'(2015), 103 .<https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-schreier.pdf> accessed 19 December 2021.
[22] PPD-21 or the Presidential Policy Directive is a US directive that deals with the strengthening of the security and ensuring protection of the states' critical infrastructure. See Cyber Security & Infrastructure Security Agency, *Critical Infrastructure Sectors* (21 October 2020) <,<https://www.cisa.gov/critical-infrastructure-sectors#:~:text=Presidential%20Policy%20Directive> accessed 26 June 2022.
[23] According to the PPD-21, Chemical industries, commercial and financial buildings, and communication infrastructure, including wired and wireless networks, satellites, voice, data, and communication service systems, are just a few examples of infrastructure that have been recognised as being vulnerable to cyberwarfare attacks. Others include dams, bases for defence, the industrial sector, emergency services, nuclear reactors, facilities for the provision of health care, information technology, energy, and government services, as well as kinetic weapons.
[24]Kyriaki Athanassouli 'Economic Implications of the Rise of the Information Warfare, Cyber War and Cyber Security', in Nicholas J Daras, (ed.) *Cyber Security and Information Warfare* (Science Publishers 2019), 39.
.

or non-intentional cyber operation against a single state may affect over 20 states indiscriminately.[25] Thus, cyber warfare is a global issue and a threat to humanity.

4.2 Combatants in cyberspace

A combatant is an individual actively participating in an armed conflict.[26] Combatants are part of an armed force[27] such as an army, volunteer corps, gang or militia. Unlike combatants, civilians, medical and religious personnel, prisoners of war, individuals displaying distinctive emblems and *hors de combat* are protected from being attacked in fields of war.[28] In cyber warfare, however, the combatants are the cyber experts who serve the purpose of launching defensive and offensive cyber operations and causing violence for political and military reasons.[29] Their activities are based on creating, designing, developing and launching defensive and offensive cyber operations.[30] In most instances, governments have been known to hire non-state actor cyber armies or private individuals to execute cyber operations as approximately 80 to 90 per cent of networks are privately owned and controlled.[31] Thus, cyber experts are normally recruited by armies to form cyber forces.

Generally, the protection of human dignity is extended to all beings with human attributes; in warfare, however, this protection is afforded to protected persons and objects only. In cyber war, it is difficult to differentiate combatants from civilians because there is one cyberspace, one shared by both civilians and combatants and it guarantees anonymity and probable deniability to its users if they require so.[32] However, even though the perpetrators are afforded invisibility, their actions may be seen and felt in the physical world. Because the actors may not be seen, it is difficult to anticipate who is to blame, his/her positioning, and

[25] International Committee of the Red Cross, *Cyber Warfare: Does International Humanitarian Law Apply?* [25 February 2021] <https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law > accessed 15 September 2022.
[26] Article 43(2), the Protocol Additional to the Geneva Conventions of 12 August 1949 relating to the Protection of Victims of International Armed Conflicts [8 June 1977] 1125 UNTS. [Hereafter referred to as Additional Protocol I].
[27] IHL [International Humanitarian Law] Database<https://ihl-databases.icrc.org/customary-ihl/eng/docindex/v1_rul_rule3> accessed 24 March 2022.
[28] For protected persons under IHL, see arts 24, 25 & 26 of the Geneva Convention I; Articles 36 & 37 of Geneva Convention II; Articles 12–16 of the Geneva Convention III; Articles 3, 20 of the Geneva Convention IV; Articles 8, 10, 12, 15 (1), 79 of Additional Protocol I; Articles 7, 9(1), 11, 13, 14 of Additional Protocol II.
[29]PJ Springer, *Encyclopedia of Cyber Warfare* (ABC-CLIO 2017),75.
[30]M Aschmann , J van Vuuren.& L Leenen,) 'Towards the Establishment of an African Cyber-Army' (2015) 14 (3)Journal of Information Warfare, 15 , <https://www.jstor.org/stable/26502728> accessed 21 March 2022
[31] James Lewis, 'Private Actors' Roles in International Cyber Security Agreements' (2022) 7 (1) The Cyber Defense Review, 33.
[32] PK Mallick, *Cyber Weapons: A Weapon of War?* Vivekananda International Foundation 2021), 5

the appropriate retaliation.[33] With this regard, an adversary in a cyber war can hardly be identified, and because of the dual use of cyber-linked infrastructure, civilians are likely to be caught in between. Civilians may thus be exposed to life-threatening danger.

4.3 Cyber weapons

Cyber weapons are computer programs capable of rendering violent implications in the physical world.[34] In the context of warfare, they include malware, tools, tactics and any other activity that can be used to execute offensive operations for military or political objectives in cyberspace.[35] Any cyber attack takes five steps to be executed. It begins with reconnaissance, which is the recognition of a target. Thereafter, a weapon is staged and prepared for the attack. Then the weapon or malware is launched and the exploitation of the computer system follows, to which computer software, hardware, other physical infrastructure, and human beings may fall victim.[36] After the installation of the malware, which is the weapon, the attacker establishes command and control of the system.[37] At this level, the attacker can manipulate the system to meet his objective and accomplish the mission. According to the *Tallinn Manual 2.0*, for a weapon to fall into the category of a cyber weapon, it must be defined as a means in cyberspace designed to be used and capable of rendering injury, destruction or death as a consequence of an attack in a cyber operation.[38] This entails that a weapon in cyberspace may become a cyber weapon in the context of cyber warfare only if it can be used to instigate violence, just as in traditional warfare.

The differences between conventional or traditional weapons of war and cyber weapons are that first, the effects of traditional weapons are irreversible, consistent, scale with volume, local and a single weapon can be used only for a single target.[39] The effects of cyber weapons, however, may be reversible, created for a specific target, variable, may be global, and a single weapon can be used against multiple targets intentionally or not.[40] It is clear, then, that the nature of weapons used in cyber warfare is unique and distinct from those used in kinetic warfare.

---

[33] cf Springer (n 29 16).
[34] ibid, 76.
[35] ibid, 173.
[36] ibid, 77.
[37] ibid.
[38] Michael N Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare.* (Cambridge University Press 2013), Rule 110. [Hereafter referred as the *Tallinn Manual 2.0*.]
[39] cf Mallick (n 32 16–17).
[40] ibid.

To protect the dignity of civilians, International Humanitarian Law rules prohibit the use of weapons that are incapable of discrimination.[41] From standpoint of technology, some cyber weapons can be developed and deployed to affect specific targets, rather than spreading or rendering harm indiscriminately.[42] However, because of the interconnectedness that characterises cyberspace, anything with an internet link can be targeted from anywhere in the globe, and a cyber attack on one system may have ramifications on other systems.[43] There is, thus, a serious danger that cyber tools cannot be developed or deployed in accordance with IHL rules to protect human dignity, either intentionally or unintentionally.

The challenge regarding the use of cyber weapons for the protection of civilians is that cyber weapons are unpredictable, and it may be difficult to make an assessment of the damage. Cyber wars are more likely than kinetic warfare to cause collateral damage. Nevertheless, the fact that cyber weapons can be deployed easily makes them more difficult to control.[44] It can thus be concluded that, the uniqueness of cyber weapons is such that it is essential that adoption the most relevant and efficient regulation pertaining to them are adopted.

5.0 IS INTERNATIONAL LAW ON THE USE OF FORCE SUFFICIENT FOR PROTECTING HUMAN DIGNITY IN CYBER WARFARE?

The fundamental tenet of the protection of humanity is what propels the humanization of international law. This point was echoed by the ICTY in the *Furundzja* case. The ICTY opined that the protection of human dignity is central to both human rights and the body of international humanitarian law.[45] Thus, the foundation of international human rights and international humanitarian law is the universal ideal of respect for human dignity. In this regard, in both processes of creating and interpreting the rules, human dignity serves as a counterbalancing element to that of military necessity.

It is indisputable that the scope of warfare has expanded beyond conventional or kinetic warfare. This expansion has brought into question the existing international law's relevance in regulating newly emerging warfare such as cyber warfare. This concern stems from the absence of a single specific and binding international law that governs the use of force in

[41] Article 51(4) of Additional Protocol I.
[42] ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts :ICRC Position Paper [November 2019] <<https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts> accessed 20th September 2022.
[43] cf Springer (n 29 68–69).
[44] cf Burkadze(n 12).
[45] *Prosecutor v. Furundzija*, T.Ch. II (10 December 1998).

cyberspace. However, despite some disagreements, there exist affirmative positions by states[46] and other international organisations such as the ICRC[47] on the relevance of the *lex lata*, or the presently enforced law. According to the ICJ, IHL rules were drafted in such a manner that they are applicable to all present and future means and methods of war.[48] With this in mind, IHL rules apply in regulating cyber warfare just as they are relevant in regulating conventional warfare.

War, by its very nature, results in dehumanization and encourages brutality. For the sake of the protection of human dignity, international law advocates for the peaceful settlement of disputes and proscribes all forms of the use of force and threats,[49] cyber aggressions included. Nevertheless, the Geneva Conventions of 1949 and protocols thereof regulate the conducts of parties in war fields. Additionally, they articulate principles that protect innocent civilians from falling victim to war atrocities. These principles include; distinction, precaution, proportion, dictates of public conscience, and humanity. Where no law provides for the protection of civilians, the 'Martens Clause' fills in. The clause provides that civilians remain protected by international law rules derived from international customary law; specifically, from the principles of the dictates of public conscience and humanity.[50] Thus, the protection of humanity in warfare is generally given priority.

Commentators and scholars are in agreement that cyber operations that render injury, death and destruction may fall within the bounds of an attack or use of force under the *jus ad bellum* or the law on the use of force.[51] Nevertheless, even though there is no express mention of cyber attacks in the Geneva Conventions, so long as those attacks qualify to fall within the ambit of a war or an armed attack, then they may qualify to be regulated under the Geneva

[46] See UN Doc/A/66/152[15 July 2011],6; UN Doc/A/65/154[July 2010], 15; UN Doc/A/57/166 [29 August 2002], 3; Kersti Kaljulaid, 'Opening Remarks on Cycon' (2019) <https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html> accessed 4 August 2022; Michael Schmitt 'Germany's Positions on International Law in Cyberspace'https://www.justsecurity.org/75278/germanys-positions-on-international-law-in-cyberspace-part-ii/> accessed4th August 2022.

[47] International Committee of the Red Cross (ICRC) 'Speech (ICRC) to the Third Session of the ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025'[22 July 2022];.<https://www.icrc.org/en/document/icts-armed-conflicts-risk-harm-civilians-civilian-infrastructure > 5August 2022> This information was also confirmed during an interview with an ICRC officer, Dar es Salaam office on 18 July 2022.

[48] International Court of Justice, *Legality of the Threat or the Use of Nuclear Weapons* (Advisory Opinion) [8 July 1996] [86].

[49]United Nations, Charter, Article 2(4), Article 33 of the UN Charter.

[50] Hague Convention. Article 1(2) of Additional Protocol I, paragraph 9 of the preamble to the 1899 Hague Convention (II); Hague Convention (IV), para 8 of the preamble to the 1907 Hague Convention (IV).

[51] See the first 20 Rules in the *Tallinn Manual 2.0* which are are on the application of *jus ad bellum* in cyber warfare. cf Schmitt (note 38).

Conventions or *jus in bello*.[52] However, looking at the nature of cyberspace, it can be agreed that, even though cyber warfare is subject to international law on the use of force, cyber warfare is clearly a segment of warfare that requires its own legally binding international framework.[53] A cyber war can hardly ensure the protection of human dignity and, additionally, some humanitarian principles can hardly be applied in the cyber war context.[54]

5.1 Weaknesses of the *lex lata* in affording protection of human dignity in cyberspace

The discussion below provides evidence for the argument that even though the conventional regime is relevant, it is not sufficient for the regulation of cyber warfare so as to afford protection to human dignity.

5.1.1 Lack of the cyber language in the *lex lata*

Technology generally has been growing very fast, inversely proportional to policies, laws and regulations. These developments culminate in the need for amendments or the adoption of new laws to fill in the gaps brought about by the new advancements. Cyber technology is one among many of these developments. The current corpus of international law on armed conflicts lacks the necessary cyber language. For example, from its analysis, the UN Charter is not cyber-centric, rather, it is more about prohibiting kinetic force which was the key purpose of its adoption.[55] The existing regime of international law does not directly refer to cyber operations as means and methods of war.[56] Cyber warfare is a broad technical and technological concept that necessitates a special and well-drafted legal framework that reflects the nature of cyberspace.

Due to the lack of a cyber language in the international legal framework regulating the use of force, it must be difficult to have a single interpretation of an armed attack in the cyber context. This is a setback to the regulation of cyber aggression and ensuring the protection of

[52] The second part of the *Tallinn Manual 2.0* comprises 70 Rules on the application of *jus in bello* in cyber warfare.

[53]Sandra L Hodkinson, 'Crossing the Line: The Law of War and Cyber Engagement – Applying the Existing Body of Law to this New National Security Threat'(2016) 51(3)*The International Law*, 613.

[54] Daniel Abebe,. 'Cyber War, International Politics, and Institutional Design' (2016) 83(1)*The University of Chicago Law Review*<https:// www.jstor. org/s table/ 43741589> accessed 20 September 2021 , 1. This information was confirmed during an interview with a senior lecturer from the University of Dar es Salaam on 21 July 2022.

[55] cf Burkadze (n 12) . This information was also stated during an interview with a legal practitioner from Right Mark Attorneys on the 20 May 2022.

[56] During the drafting of the UN Charter the question on the scope of the term 'use of force' ignited a scholarly debate. It was then concluded that the prohibited force in the UN Charter is only that which involves armed force and not otherwise. Thus, to incorporate the regulation of use of force into cyberspace, the provision must be interpreted broadly. Nevertheless, although the Geneva Conventions clearly recognise land, water, airspace and outer space (physical realms) as fields of war, there is no mention of cyberspace.

human dignity. The existing loopholes can be used by perpetrators as a scapegoat to justify their crimes. Furthermore, under international criminal law and the humanitarian legal framework, no law provides a clear-cut wording on what acts may constitute grave breaches or war crimes and crimes against humanity in cyberspace. Lack of cyber language in the realm of international criminal law may incite impunity and the continuous violations of human dignity in cyberspace.[57] Even though the *lex lata* does not refer to cyber terms in the international security context, international law in the cyber realm may develop progressively through practice. This is, however, yet to be visualised because there is yet no general practice in the regulation of cyber warfare. In reality, thus, the international law on the use of force provides inadequate protection to civilians.

5.1.2 Interpretative problem

From the analysis of the legal framework regulating the use of force, it is revealed that the interpretation problem is rooted in the lack of cyber language in most of the major conventional bodies regulating warfare.[58] This problem may be the key factor for diverse arguments on the applicability of international law in regulating cyber aggression. Even though the *Tallinn Manual 2.0* has illustrated how the *lex lata* may be interpreted in the context of cyber warfare, it has been criticised severally for several reasons and also because it does not provide the declared position of states, but rather the views of some experts sponsored by NATO.[59]

The application of a legal provision depends on how one interprets it.[60] There are three approaches to legal interpretation. One is textual, which considers the text as it is; the second approach focuses on the aim of the parties to that particular treaty; and the third focuses on the objective of the adoption of the treaty by the parties or drafters.[61] In the first approach, and considering Article 2(4) of the UN Charter, the term 'use of force' is restrictive only to armed force. This approach, thus, *excludes* a number of cyber aggressions from the bounds of the use of force, such as attacks on banking and other economic systems and cyber espionage, just to mention a few. If one interprets the same provisions in an intentional or objective

[57] cf Burkadze (n 12).
[58] ibid.
[59] Michael Schmitt 'Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't (9 February 2017) <https://www.justsecurity.org/37559/Tallinn-manual-2-0-international-law-cyber-operations/> accessed 28 June 2022.
[60] Mark Greenberg , 'Legal Interpretation' in *The Stanford Encyclopaedia of Philosophy*, E Zalta (ed.) <https://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=legal-interpretation> accessed 16 October 2022 A similar argument was raised during an interview with a legal practitioner from Right Mark Attorneys in Mwanza on 20 May 2022.
[61] Vienna Convention on the Law of Treaties, art 31 of the 23 May 1969.

approach, a conclusion will be drawn that the provisions are relevant in regulating cyber warfare. This is because the objective of the establishment of the United Nations is to address all forms of aggression that threaten international peace and security,[62] hence the adoption of the United Nations Charter. Thus, currently the extent to which IHL regulates cyber operations depends on how states interpret current IHL regulations.

5.1.3 The virtual nature of cyberspace

The regulation of armed activities in cyberspace is more technical as compared to the regulation of conventional warfare on the physical field. These technicalities are aligned to the unique features of cyberspace, which pose a challenge to its regulation. It is difficult to identify an attacker in cyberspace.[63] The cyber warriors are like ghosts. The cyberspace is boundaryless, attacks between specific countries may have widespread effects and it is not easy to identify the actual perpetrator,[64] because it is difficult to identify the creator of malware or a piece of code: it could be typed anywhere by anyone and the adverse effects may be felt anywhere. In consequence, the technicalities pose a challenge to attribution.[65] Considering that cyberspace provides a hideout for perpetrators, who is to blame in a cyber war? The non-identifiability of a perpetrator is generally a challenge in the investigations into and the prosecution of crimes committed in cyberspace.[66] Nevertheless, in a circumstance in which both the perpetrator and purpose of the attack are unknown, it is difficult to anticipate which law is applicable, whether domestic, criminal, or international law.

5.1.4 The 'state responsibility' notion

The law on the non-use of force, in particular the United Nations Charter, concentrates on prohibiting the use of force by states alone, thereby exempting non-state actors.[67] This finding is in consideration of the fact that cyberspace is intangible; it is made up of software, hardware and data which are mostly not state-owned *per se*, but are rather under the control of private entities.[68] Thus, states seek assistance or employ private cyber actors.[69] With this

[62] United Nations, Charter arts 1 and 2.
[63] cf Springer (n 29 75).
[64] cf Mallick (n 32).This information was confirmed during an online interview with a cyber security analyst and consultant from Cyber Security Centre for Southern Africa on the 19 June 2022.
[65] Winnona DeSombre and others *A Primer on the Proliferation of Offensive Cyber Capabilities* Atlantic Council(2021) <http://www.jstor.org/stable/resrep30741> accessed 17 October 2022.
[66] This information was obtained during an online interview with a legal officer from the UN Residual Mechanism for Criminal Tribunal (IRMCT) on 16 July 2022.
[67] The Charter recognizes only states as actors, this is depicted from most of the wordings of the Charter. The Charter does not recognise non-state actors in the scope of the prohibition of the use of force.
[68] Paul J Springer, *Cyber Warfare: A Documentary and Reference Guide* (Greenwood, 2020), 22.

regard, the notion of state responsibility demonstrated in different international laws regulating warfare, exempting non-state actors, is of less relevance in cyber warfare. The state responsibility notion that is upheld in a number of international legal instruments may be challenging in the context of cyber warfare because non-state actors are more capable of fuelling aggressions in cyberspace and, in many instances, states are likely to involve non-state actors as cyber warriors to execute violent cyber attacks.[70] Private entities and individuals are the major actors in cyberspace. However, the conventional regime, the United Nations Charter in particular, recognises and regulates state actors only.[71] This is detrimental to the protection of human dignity in cyberspace, as the use of force by individuals and proxies may remain unchecked.

5.1.5 Limitation on the scope of the term 'use of force' in the *lex lata*

The *lex lata* focuses its prohibition on physical force or armed force. In the *travaux preparatoires* of the United Nations Charter, it was concluded that the use of force prohibited under international law is that which is related to armed attacks that can have an impact on the physical world.[72]The study found that there are some cyber aggressions capable of being termed as use of force, but they do not fit within the context of the use of force provided in the *lex lata*. Cyber technology has evolved, bringing with it new devastating threats that are capable of crippling the financial and banking systems of a state. It is capable of rendering atrocious economic devastation that may leave many civilians in misery. Economic devastation and subjection to poverty is a violation of human dignity. Furthermore, economic force may pose a serious threat to the political sovereignty of a state and its diplomatic relations with another state.

The concept of economic coercion is not within the definition provided for in the *lex lata*. In other words, under the conventional regime, economic force does not constitute the use of force. However, literature provides that traditional economic pressure cannot be likened to situation in which today's cyber capabilities are able to bring about the economic downfall of

[69] cf Lewis (n 31).
[70] This information was obtained during an interview with a legal practitioner from Right Mark Attorneys on 20 May, 2022.
[71] The UN Charter addresses UN member states and not individuals or private entities. Refer to art 3(1) of the UN Charter.
[72] Considering art 2(4) of the UN Charter in the textual interpretation approach, the term 'use of force' is restrictive only to armed force. Thus, this approach excludes a number of cyber aggressions from the bounds of the use of force, such as attacks on banking and other economic systems and cyber espionage, just to mention a few.

a state.[73] With current technological developments, economic force may grow into an armed conflict in the cyber context,[74] yet the *lex lata* does not recognise it as a use of force. Thus, the conventional framework is insufficient in regulating all forms of cyber aggression in affording total protection of human dignity.

5.1.6 Challenges in regulating cyber weapons

The technology used in developing and designing cyber weapons is less complicated compared with that used in the making of conventional arms such as nuclear weapons, guns, and bombardments. To develop a cyber weapon, one basically needs intellectual skills.[75] Unlike kinetic weapons, computer malware is simply a code, easy to transport, easy to launch, easy to refute responsibility for and difficult to trace or recognise.[76] The intellectual abilities or knowledge required to create cyber weapons are more valuable than the weapons themselves.

It is easy, therefore, for a state to refute ownership or possession of cyber weapons, but it may invest in cyber weapon-making skills.[77] And even if the state does not invest in cyber weapon-making skills, private entities may fill the gap. In this regard, the current conventional methods are not sufficient in limiting the creation and use of cyber weapons because, generally, cyber weapons cannot be inspected, identified or even monitored. Thus, even though the current conventional framework on the use of force has been affirmed by many to apply to all forms of inter-state aggression, it is not sufficient to regulate cyber warfare and assure civilian's security. Due to this, protection of human dignity may require restraint of the proliferation of cyber weapons.

5.1.7 Humanitarianised interpretation of war concepts in a cyber context

The principle of humanity is a normative-ideational principle that reflects the ideals embodied within the concept of human dignity.[78] Because the objective of International Humanitarian Law is to protect humanity,[79] concepts relative to warfare in cyberspace should be interpreted in such a manner that the protection of human dignity can be afforded and human life is valued. These concepts include violence, use of force, self-defence and armed

[73] Chiluba Edo 'The Use of Force and its Impacts on the Economic Growth of States under International Law' (2021) <https://sssrn.com/abstract=3971290> accessed 17 October 2022
[74] cf Springer (n 68).
[75] cf Mallick (n 32 38).
[76] ibid.
[77] cf Springer (n 68 71,75).
[78] cf Shaoping & Lin (n 6).
[79] United Nations, Charter, Preamble.

attack, just to mention a few. Furthermore, the humanitarian principles should be interpreted in a manner that reflects the nature of cyberspace and cyber aggressions.

It is generally accepted that, in determining the use of force, the best approach to defining the term 'armed attack' is based on the rationale and effects emanating from the attack.[80] Under the *Tallinn Manual 2.0* and the law on the use of force, specifically the United Nations Charter, attacks that do not cause physical consequences are not regarded as armed attacks, regardless of any other effects that a state or civilians might suffer. In the cyber context, the effects should not be limited to physical effects. This is because, unlike cyber attacks, the effects of a kinetic attack can easily be depicted physically through injuries, deaths and destruction of property. In cyber warfare, however, some effects may be felt but not seen, and there may be no physical violence or destruction at all. Thus, the interpretative shift is necessary to accommodate the protection of human security, state and peace in cyberspace.

It is evident that the United Nations Charter forbids the use of force, but it does not specify the breadth or depth to which force may amount to the illegal use of force under international law. Fortunately, scholars have made attempts to provide a clear understanding of cyber war ever since it first emerged. In line with this, the group of experts who drafted the *Tallinn Manual 2.0* provided a number of factors which may characterise an interstate cyber act as falling within the ambit of the use of force. These factors include: severity, immediacy, directness, measurability, military nature, state involvement and presumed legality.[81] In this regard, there are instances where cyber operations fall within the threshold of the use of force. To protect humanity, the concept of the use of force and violence or armed attack, should be expanded to include non-physical consequences. For example, Article 51(2) of the Additional Protocol I, forbids attacks that may cause psychological torture in the form of terror.[82] Article 54 prohibits acts that may destroy, remove or cause objects that are indispensable to the survival of civilians to be useless.[83] These provisions should apply similarly to cyber aggression.

Nevertheless, the definition of the protection of civilian objects should be extended to the definition of civilian data or information found in cyberspace, such as data in civilian hospitals and data in financial institutions, just to mention a few. Such data is essential in

[80] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v The United States of America)* ICJ Rep 1986, para 195.
[81] *Tallinn Manual 2.0*, 47–52.
[82] Geneva Convention, art 51(2) of Additional Protocol I.
[83] ibid, Article 54.

different facets of civilian well-being. Erasing or manipulating vital civilian data can easily affect commercial businesses and even halt the provision of essential services. Such actions may jeopardize the lives of civilians more than they can destroy physical objects.

6.0 CONCLUSION

In conclusion, due to the speed of technological advancements, it is apparent that cyber warfare is indeed the future prospect of war. Technological advancements have substantially altered, not just the nature of wars, but also the understanding of the concept of the armed attack itself. The *lex lata* on the use of force has been accepted to be relevant in regulating cyber warfare but it is not sufficient. It is appropriate, thus, that cyber threats call for a new international legal infrastructure since the framework currently in place is too obsolete to address the current conflict-related problems. This study recommends the following:

First and foremost, is the adoption of an additional protocol to the Geneva Convention relative to the protection of civilians in cyber war. This is because the existing legal framework is, as discussed, insufficient. The new protocol should address cyber threats and regulate cyber weapons. It should also include definitions of common cyber war concepts for clarity and for determining the extent to which cyber aggression may constitute the use of force. This protocol should explain how international law principles could be applied in cyber warfare. Furthermore, the framework should prioritise respect for human dignity to assure the protection of innocent civilians.

Furthermore, international cooperation in addressing cyber warfare should be strengthened. The significance of international cooperation in addressing cyber aggressions is based on the fact that cyberspace lacks definite boundaries and no nation is immune to cyber attacks. It is a realm that runs beyond international borders: it is, therefore, an international issue. Joint monitoring and defence mechanisms should be established among states. In other words, cyber warfare should be addressed through dialogue and treaty agreements. The unified efforts should advocate for the peaceful use of the virtual space.

States' accountability for the desecration of international law should be promoted. Through dialogues, the United Nations should establish legal and technical standards for attribution in instances where states commit international wrongful acts in cyberspace. Additionally, it should establish and strengthen lawful responses that hold perpetrators accountable and deter others from violating international law and the principles thereof. The United Nations General Assembly should preach accountability and adherence to international norms and standards in cyber space.

Just as it plays a big role in addressing kinetic conflicts, the United Nations Security Council should act similarly in responding to cyber warfare by enhancing cyber peacekeeping. The Security Council should take the lead in determining the persistence of threats or aggression instigated in cyberspace. In that case, it should prevent the cyber conflict from backfiring, by deploying digital cyber peacekeeping forces who are able to prevent escalation of the effects of the cyber attacks and help party states reach peaceful agreements. The peacekeeping forces should be comprised of experts in cyber technology and cyber diplomacy. They should be capable of monitoring actions in cyberspace that desecrate peace agreements. They should be capable of demobilising cyber combatants, addressing the disarmament of cyber weapons, offering mitigation measures to victim states, ensuring non-violation of human rights in cyberspace and overseeing cyber peace agreements and the end of a cyber war.

At the domestic level, mitigation practices should be bolstered. Under the responsibility to protect (R2P), states have the duty to protect their people from harm and threats. With this regard, governments should take initiatives to promote security in critical infrastructure that are dependent on software to operate. The initiatives should include the prevention, protection, investigation, mitigation, response and recovery from cyber attacks. The measures should include building and strengthening of military cyber units with capabilities in cyber defence, launching cyber attacks and cyber intelligence. This should go hand in hand with raising cyber awareness, training and recruiting experts in cyber technology and cyber law.