THE LAW OF ARMED CONFLICT IN THE ERA OF CYBER TECHNOLOGY: ASSESSING THE LEGAL CHALLENGES AND RESPONSE IN TANZANIA

Petro Protas[*] and Leonard Chimanda Joseph[**]

Abstract

The development of cyber technology has brought challenges to various aspects of life. Legal regime regulating the means and methods of warfare stands amongst the most affected regimes due to such advancement. The existing puzzle is on whether there is a need to conclude a new Convention on international humanitarian law to address the challenges of cyber technology or not. While discussing issues relating to this puzzle, this article examines the legal regime in Tanzania and its rapport to the rules of international humanitarian law (IHL) including cyber warfare. The article observes out that, the Tanzanian legal framework insufficiently addresses the challenges of cyber warfare. Apart from relying on the ordinary crimes approach in interpreting and prosecuting IHL breaches, this article concludes that necessary legislative measures need to be taken by Tanzania to fill the gaps brought by cyber technology to the rules of IHL.

Keywords: *Armed Conflict, Cyber Technology, Cyber Warfare, Law of Armed Conflict, Ordinary Crimes Approach, Tallinn Manual.*

---

[*] Mr. Protas holds LL.B (Hons) and LL.M from the University of Dar es Salaam, Dip. Legal Practice (LST), Ph.D Candidate (University of Dar es Salaam); Assistant Lecturer, University of Dar es Salaam School of Law; He may be contacted *at petro_protus@yahoo.com*or*protas.petro@udsm.ac.tz*

[**] Mr. Leonard holds LL.B (Hons) and LL.M from the University of Dar es Salaam. He is currently an Assistant Lecturer at the University of Dodoma. He may be contacted at *leonardchimanda@gmail.com*

1. INTRODUCTION

Warfare has never been a static concept. Throughout human history, this concept has been changing and camouflaging itself within technological advancement and the rise of varying political ideologies.[1] It is not a surprise that scholars such as Carl von Clausewitz compare 'the warfare concept to a true chameleon, ever-changing to adapt to new circumstances'.[2] For instance, in ancient times, man used stones, swords, arrows, and shields as weapons of war.[3] Over time, the importance and usefulness of these means of warfare became insignificant due to evolving circumstances and development in human technology. The rise of new means of warfare and extremist political ideologies[4] in the 20th century saw more ruins than the preservation of human life. Poisonous gas,[5] atomic bombs,[6] chemical[7] and other weapons

---

1 AALCO, "Cyber Warfare and International Law", in AALCO, *International Law in Cyberspace*, New Delhi: AALCO, 2017, p. 73, at pp.73-74. See also Palmieri, D., "How Warfare has Evolved – A Humanitarian Organization's Perception: The ICRC, 1863-1960", 97(900) *International Review of the Red Cross*, 2015, pp. 985-998, at p. 985.

2 Von-Clausewitz, C., *On War*, New Jersey: Princeton University Press, 1984, at p. 89. See also Bernard, V., "Tactics, Techniques, Tragedies: A Humanitarian Perspective on the Changing Face of War", 97(900) *International Review of the Red Cross*, 2015, pp. 959-968, at p. 959.

3 Molloy, B.P.C., "Hunting Warriors: The Transformation of Weapons, Combat Practices and Society during the Bronze Age in Ireland", 20(2) *European Journal of Archaeology*, 2017, pp. 280-316, at p. 283.

4 See for instance the rise of Nazism in German and extermination in camps in Hicks, J., "Too Gruesome to be fully Taken in: Konstantin Simonov's the Extermination Camp as Holocaust Literature", 72(2) *Russian Review*, 2013, at pp. 242-259.

5 See Padley, A.P., "Gas: The Greatest Terror of the Great War", 44(1) *Anaesthesia and Intensive Care*, 2016, pp. 24-30, at p. 24.

6 See Press, D.G., Sagan, S.D., and Velentino, B.A., "Atomic Aversion: Experimental Evidence on Taboos, Traditions and the Non-Use of Nuclear Weapons", 107(1) *The American Political Science Review*, 2013, pp. 188-206, at p. 188. See also Groom, A.J.R., "U.S-Allied Relations and the Atomic Bomb in the Second World War", 15(1) *World Politics*, 1962, pp. 123-137, at p. 124. See also Malloy, S.L., "A Very Pleasant Way to Die: Radiation Effects and the Decision to

which had indiscriminate effects on human population were used during armed conflicts. The battlefields became more deadly and inhumane than they were during ancient times. No sooner had the international community addressed the challenges brought by the aforementioned means than the development of cyber technology took place. Just like other advancements, cyber technology has brought immense challenges to the very concept of warfare.

Through a computer system both military and civilian objects can be severely paralyzed, leaving similar or higher physical effects to human beings, environment, and cultural heritage than it is for kinetic warfare.[8] This Article, therefore, highlights the challenges brought by the advancement of cyber technology and its synergy to the rules of international humanitarian law (IHL). It also reveals the global efforts directed towards addressing the emerging challenges as well as the legal response by Tanzania. To achieve this aim, the article discusses in details, the historical evolution of means and methods of warfare, the concept and challenges of cyber warfare, the law of armed conflict in Tanzania, the status of domestication of the laws of war and its effects in Tanzania and, finally, the response of the Tanzanian legal framework in so far as cyber warfare is concerned.

Use the Atomic Bomb Against Japan", 36(3) *Diplomatic History*, 2012, at pp. 515-545.

7 Faith, T., "It Would be Very Well if We Could Avoid it: General Pershing and Chemical Warfare", 78(3) *Historian*, 2016, pp. 469-485, at p. 469.

8 AALCO, *Cyber Warfare and International Law*, above note 1, at p. 74.

2. HISTORICAL CONTEXT: MEANS AND METHODS OF WARFARE

The phrases 'means of warfare' and 'methods of warfare' are very common in the field of international humanitarian law. Generally, means of warfare refer to the variety of physical means, including weapons and weaponry systems, employed to inflict damage to the adversary during military operations.[9] On the other hand, the phrase –"methods of warfare" encompasses all tactical or strategic procedures the purpose of which is to weaken or outweigh the enemy on the battlefield.[10] Deportation,[11] pillage,[12] use of human shields,[13] employing perfidious acts,[14] taking of hostages,[15] reprisals against protected persons,[16] and denial of a quarter or refusing to spare lives of protected persons are some examples of prohibited methods of warfare regulated under International Humanitarian Law [IHL] rules.[17]

---

9 ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1997*, Geneva: ICRC, 2006, at p. 937.

10 Ibid.

11 Article 49 of the Convention IV – Convention Relative to the Protection of Civilian Persons in Time of War, 1949. See also Article 17 of Additional Protocol II – Protocol Additional to the Geneva Conventions, 1949 relating to the Protection of Victims of Non-International Armed Conflicts, 1977. See also Rules 129 and 130 of the ICRC Customary International Humanitarian Rules, 2006.

12 Article 33 (2) of Geneva Convention IV. See also Article 4 (2) (g) of Additional Protocol II.

13 Article 51 (7) of Additional Protocol I. See also Rule 97 of the ICRC Customary International Humanitarian Rules, 2006.

14 See Article 37 and 39 (2) of Additional Protocol I.

15 Article 34 of the Geneva Convention IV. See also Common Article 3 to all Geneva Conventions. See also Article 75 of Additional Protocol I.

16 See Articles 51 (6) and 52 (1) of Additional Protocol I. See also Rules 145 to 148 of the ICRC Customary International Humanitarian Rules, 2006.

17 For denial of quarters see Article 40 of Additional Protocol I.

Ordinarily, the means and methods of warfare that cause superfluous and unnecessary suffering to human beings and the human environment are strictly prohibited under IHL.[18] The deployment of these means or methods of warfare should aim only at weakening the military capacity of the adversary while offering a military advantage to the attacker.[19] Additionally, the law of war requires States to consider whether their study, development, acquisition, or adoption of new weapons, means or methods of warfare, would be in some or all circumstances, prohibited on the battlefield.[20] If their determination is positive, such an innovation should not be carried out or should be modified to confine itself within the requirement of the law.

Historically, means and methods of warfare have been in constant evolvement due to the advancement of technology and the changes in societal political ideologies.[21] The advancement of means and methods of warfare touched both their quality and effectiveness in the combat zone. This created a huge gap between the ancient and modern weapons employed on the battlefield.

For instance, during 'Stone Age' most weapons were made up of stones and hence could not offer many advantages to war

---

[18] See rule 70 of the ICRC Customary International Humanitarian Rules, 2006, Preamble to the Saint Petersburg Declaration of 1868, rule 23(e) of the Hague Regulations of 1899, article 35(2) of the Additional Protocol 1 of 1977 and article 6(2) of the 1980 Protocol II to the Convention on Certain Conventional Weapons. Additionally see also article 16(2) of the Oxford Manual of Naval War of 1913.

[19] See articles 52 and 51(5) (b) of the Additional Protocol 1 of 1977 and rule 43 of the ICRC Customary International Humanitarian Rules, 2006.

[20] See Article 36 of Additional Protocol I.

[21] See Palmieri, *How Warfare has Evolved – A Humanitarian Organization's Perception*, above note 1, at p. 985.

warriors on the battleground.[22] With less advancement in technology, the tactics of warfare highly depended on the geographical location, climate, and topographical nature of war zones.[23] Being located near mountains, ocean, or within artificially created walls[24] could offer a military advantage to an occupant society and a military disadvantage to the opponent. Such locations made it almost impossible for intruders to invade the inhabitants or infiltrate their walls.[25] Similarly, during the 'Iron Age' -1500 BC to 100 AD - weapons of war continued to be less sophisticated but more advanced than those of the Stone Age.[26] It should be noted that Iron Age marked the beginning of the revolution of means and methods of warfare.[27] Through it, later developments such as effective use of gun powder in the 1330s,[28] advancement in artillery weapons, deployment of guided torpedo, inventions of mines as well as improvement of naval and air weaponry became a reality.[29] More other developments were seen during the two world wars of 1914-1918 and 1939 -1945

---

22 Guilmartin, J.F., "Military Technology", *BRITANNICA*, available at https://www.britannica.com/technology/military-technology (accessed 15 December, 2019).

23 Ibid. See also Musso, M., *Mukwavinyika Mwamuyingana Kabila Lake la Wahehe*, Dar es Salaam: Dar es Salaam University Press, 2011, at pp. 82-99. In this book the author shows that during pre-colonial Tanganyika, the Hehe Tribe had also used topographic nature of their area to gain war advantage against their enemies.

24 See for instance the creation of Walls of Jericho at around 8000 BCE in Bar-Yosef, O., "The Walls of Jericho: An Alternative Interpretation", 27(2) *Current Anthropology*, 1986, at pp. 157-162.

25 Ibid.

26 Gabriel, R.A., and Metz, K.S., "A Short History of War: The Evolution of Warfare and Weapons", New York: Institute U.S Army War College, 1992, at p. 1.

27 Georganas, I., "Weapons and Warfare in Early Iron Age Thessaly", 5(2) *Mediterranean Archaeology and Archaeometry*, 2005, at pp. 63-74.

28 Beauregard, C., et al, "The Armaments of the Hundred Years' War and Their Effects on Western Europe", Bachelor of Science Interactive Qualifying Project Report, Worcester Polytechnic Institute, 2018, at p. 22.

29 Gabriel and Metz, *A Short History of War*, above note 26, at p. 89.

respectively. The use of machine guns, poisonous gas, chemical weapons, military tanks, anti-tanks, anti-aircrafts, and nuclear bombs dominated the battleground.[30] All these technological advancements caused the law of war to be revisited and where necessary new rules were adopted.

Currently, the battlefield and IHL rules are yet again tested with the emergence of cyber technology and its synergy to cyber warfare. It is now possible to use a small number of people operating a computer system and cause enormous damage to an enemy in a similar or even higher magnitude than the one caused in kinetic warfare.[31] Despite various discussions at the international level, on how to address the challenges of cyber warfare, still, no clear consensus has been reached. That is why it is prudent to look at cyber warfare and its emerging issues or challenges before embarking on the legal response by Tanzania.

3. CYBER WARFARE AND ITS EMERGING ISSUES

Traditionally, land, sea, air, and outer space are the main four domains of the battlefield.[32] Currently, the world is witnessing the emergence of cyberspace as the fifth domain of warfare.[33] Unlike the four traditional domains, there are uncertainties regarding the applicability of the law of warfare in cyberspace. The former President of the United States of America (USA), Barack Obama

---

30 See the use of the military tank nicknamed "T-34" by the Russians in McFadden, D.F., "Two Ways to Build a Better Mousetrap", Ohio: Ohio State University, 2000, at p. 11.

31 De Castro, N., "Modern Warfare: Is the Revolution of Weaponry Worth the Cost?" 8(16) *Undergraduate Review*, 2012, at p. 90.

32 AALCO, *Cyber Warfare and International Law*, above note 1, at p. 74.

33 Ibid.

even described cyberspace as "the wild, wild west"[34] to mean there are almost non-existent international rules to govern this domain despite its eminent presence and threats.[35]

Some of the emerging challenges include the definition of the term 'cyber warfare' itself. To date, there is no universally accepted definition of the term 'cyber warfare'. Nevertheless, the term is used to refer to warfare conducted in cyberspace by employing means and methods of warfare emanating from the advancement of cyber technology.[36] It also includes cyber operations as means and methods of warfare conducted in the context of armed conflict.[37] In international armed conflict (IAC), the term cyber warfare has been described as the actions of a certain nation to penetrate another nation's computer or network system and disrupt or damage it for military purposes.[38]

In contrast, the term 'cyberspace' is explained to mean a globally interconnected network system consisting of digital information and communication infrastructure such as the internet, telecommunication networks, computer systems, and information resident therein.[39] Therefore, cyber-attacks are normally directed to essential cyber networks connected to sensitive systems or infrastructures of a country such as dams, aircraft control, nuclear

---

34 Macak, K., "This is Cyber: 1+3 Challenges for the Application of International Humanitarian Law in Cyber Space", Exeter Centre for International Law, Working Paper Series, 2019/2, at p. 2.

35 Ibid.

36 Melzer, N., *Cyber Warfare and International Law*, UNIDIR Resources, 2011, at p. 3.

37 ICRC, "International Humanitarian Law and Cyber Operations during Armed Conflicts", ICRC Position Paper, 2013, at p. 6.

38 Clarke, R.A., *Cyber War: The Next Threat to National Security and What to Do about It*, New York: Harper Collins, 2010, at p. 32.

39 Melzer, *Cyber Warfare and International Law*, above note 36, at p. 4.

plants, electricity, and other systems that highly depend on a computer network.[40] Due to the nature of these attacks, civilians tend to experience incidental harm such as disruption of medical services, water supply as well as electricity.[41] It is crucial to point out that cyber-attacks are normally effected via sending, spreading, or transmitting malware programmes the result of which is to block the smooth operation of computer systems of the attacked State.[42] These computer malware programmes may be in the forms of viruses, worms, or Trojan horses.[43] From the ongoing discussion, one may note that the concept of 'cyber warfare' is nowhere close to that of armed conflict provided for under the Geneva Conventions and their additional protocols. In these instruments, armed conflict is said to exist when two or more states resort to the use of arms to resolve their dispute.[44] This leaves questions on whether 'cyber warfare' is also covered under this definition or whether the virus attack is equivalent to an armed attack or at what point in time will the actions of non-state actors be attributed to States.

3.1 The Global Efforts through the Prism of Tallinn Manual

The absence of a binding international instrument on cyber warfare is among the modern-day challenges relating to the

---

40 ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, above note 37, at p. 1.

41 Ibid.

42 Balthrop, J., *et al*, "Technological Networks and the Spread of Computer Viruses", 304(5670) *Science,* 2004, pp. 527-529, at p. 527.

43 Knopova, E., "New IHL Framework for Cyber Warfare", Master Thesis, Charles University in Prague, 2016, at p. 21.

44 See Article 2 (1) of Geneva Convention I. See also Article 1 of the Hague Convention Relative to the Opening of Hostilities, 1907, See also Kuper, J., *Military Training and Children in Armed Conflict: Law, Policy and Practice*, Martinus Nijhoff Publishers, 2005, at p. 10.

development of cyber technology. This continues to be an obstacle towards global efforts to achieve a binding instrument on cyber warfare. The most notable effort was initiated by the USA and the North Atlantic Treaty Organization - NATO in the year 2013 which ended up with the successful creation of a non-binding document titled 'the Tallinn Manual[45] on the International Law Applicable to Cyber Warfare'.[46] The document was prepared by a group of twenty independent practitioners and experts in cyber conflicts. Although the document is commended for being a step towards having a specific international instrument on cyber warfare, it has also attracted several criticisms.

First; the legitimacy, neutrality, and acceptability of the Tallinn Manual is doubtful. This is because its preparation was under the sponsorship of NATO. Thus, the perception of bias against it goes without saying. Secondly, the conclusion reached by Tallinn Manual that the existing IHL legal framework sufficiently accommodates cyber warfare is also challenged.[47] Such a conclusion does away with the need to conclude an international instrument to regulate issues of cyber warfare. Perhaps one may argue that this conclusion ensures that cyber warfare goes unregulated for the benefit of the NATO countries majority of which have an interest in using cyber technology as a means and method of warfare. Additionally, the conclusion reached in Tallin Manual ignores the unique features of cyber warfare which

---

45 The Manual was called 'Tallin Manual' because it was drafted by the group of twenty experts on international law who were invited by the NATO – Cooperative Cyber Defence Centre of Excellence based in the Tallin City of Estonia.

46 Tallin Manual on the International Law Applicable to Cyber Warfare, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge: Cambridge University Press, 2013.

47 Knopova, *New IHL Framework for Cyber Warfare*, above note 43, at p. 36.

obviously the contemporary IHL framework does not address. This Article acknowledges the applicability of the existing rules of IHL to incidences of cyber warfare but argues that the rules do not adequately address all challenges of cyber warfare. Thus, studying the uniqueness of cyber warfare and come out with specific legal rules is an inevitable task.

The position that the current IHL rules apply to cyber warfare is not an invention of the Tallinn Manual and this article. That position is shared by the International Court of Justice (ICJ) as well as the International Committee for the Red Cross (ICRC). In the Nuclear Weapons Advisory Opinion, the ICJ insisted that articles 2 (4), 42, and 51 of the United Nations Charter apply to all circumstances of use of force within the confines of the Charter regardless of the kind of weapons used.[48] It added further that States are prohibited from employing weapons that cannot distinguish between military objectives and civilian objects.[49] Therefore, any cyber-attack which has an indiscriminate effect on the population is prohibited during armed conflict.[50] Additionally, in its position paper of 2019, the ICRC affirms that the current IHL framework applies to cyber operations during armed conflict.[51]

---

48 ICJ, "Legality of the Threat or Use of Nuclear Weapons" Advisory Opinion, 1996, at para. 39.

49 Ibid, at para. 78.

50 See Dinstein, Y., "The Principle of Distinction and Cyber War in International Armed Conflicts", 12(2) *Journal of Conflict and Security Law*, 2012, at p. 262.

51 ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, above note 37, at p. 6.

3.2 The Existing IHL Framework vis-à-vis Cyber Warfare

Cyber warfare has several unique features that differentiate it from kinetic warfare. Such features have brought several challenges to the existing IHL framework as follows:

There is a difficulty in establishing the applicability of IHL to cyber warfare especially when cyber warfare is not accompanied by kinetic warfare. Normally, the rules of IHL are applicable during either an international armed conflict (IAC) or a non-international armed conflict (NIAC).[52] For both IAC and NIAC[53] to exist there should be a resort to the 'use of arms' as a way of resolving the differences between the parties to the conflict.[54] Hence, the presence of 'armed attack' is a necessary ingredient for the existence of armed conflict under the rules of IHL.

A question arising is whether 'cyber warfare' or 'cyber-attack' constitutes armed attack within the meaning of IHL rules. The answer to this question is not found in any treaty law. However, experts have opined that the determination of a cyber-attack as an 'armed attack' depends on the scale of the attack and its effects.[55] Others have opined that if a cyber-attack has occasioned the

---

[52] See Articles 2 and 3 of the Geneva Conventions of 12 August, 1949, articles 1(4), 96(3) of Additional Protocol I, and article 1(1) of Additional Protocol II.

[53] IAC involves the resort into the use of arms between two or more states where as NIAC is an armed conflict between a state and dissident armed group (s) or between one or more armed groups in the territory of a particular state. For more details see ICTY, *Prosecutor v. Dusko Tadic*, Decision on the Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995, at para 70. See also ICTR, Prosecutor v. Jean Paul Akayesu, Case No. ICTR-96-4-T, at para. 602.

[54] ICRC, "How is the Term 'Armed Conflict' Defined in International Humanitarian Law?", International Committee of the Red Cross Opinion Paper, 2008, at p. 5; see also ICTY, *Prosecutor v. Dusko Tadic*, Decision on the Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995, at para 70.

[55] Tallin Manual, above note 45, at p. 53.

same effects as a kinetic force, such as death, injury, or destruction that an attack should qualify as an armed attack.[56] This view has been rejected by the ICRC on the ground that; "interpreting cyber-attack as applying only to incidences of death or injury may end up excluding other significant harms to civilian networks such a communication, banking or electricity".[57] The ICRC, therefore, urges States to find out a common understanding aimed at adequately protecting civilians against cyber-attacks.[58] It is insisted in this article that even if a common understanding is reached regarding cyber-attacks as armed attacks, still other gaps will continue to exist. For instance, in the Geneva Convention III and Additional Protocol I, for combatants to be recognized as lawful, some of the requirements that must be met are the carrying of arms openly and wearing of distinctive signs identifiable from a distance.[59] These requirements are hardly met by operators or persons launching cyber-attacks.

Additionally, there are difficulties in holding States responsible for cyber-attacks originating from their territories. This is due to the reality that most cyber-attacks are done anonymously.[60] The authors of cyber-attacks hardly reveal their identity or location of the attack.[61] In case the attacker has been identified, it becomes problematic to attribute the actions of the attacker to a particular

---

56 See Schmit, M., *Cyber Operations and the Jus in Bello: Key Issues,* Naval War College International Law Studies, 2011, at p. 15.

57 ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, above note 37, at p. 8.

58 Ibid.

59 See Article 4 of Geneva Convention III. See also Article 43 (2) of Additional Protocol I.

60 Greppi E., *International Humanitarian Law in Cyber Operations*, Italian Institute for International Political Studies, 2018, at p. 2.

61 Knopova, *New IHL Framework for Cyber Warfare*, above note 43, at p. 41.

State. Accused states have always distanced themselves from cyber-attacks insisting that they have been launched by private entities or other States.[62] For example, in 2007 Russia denied responsibility for Estonia's cyber-attack by arguing that it was launched from her territory but by private persons.[63] Also, it is difficult to explain the territorial aspect of cyber warfare in line with the existing IHL rules. IHL provides for the so-called "zone of operations of a belligerent".[64] Cyber-attacks are normally carried out without the need to occupy a particular territory of the attacked State. With this unique feature, it becomes impossible to establish zone(s) to territory controlled by an adverse party.

Moreover, observing the principle of distinction in cyber warfare is a challenge.[65] In practice, computer networks used by civilians and the members of the military are normally closely interrelated (dual-use purposes).[66] This makes it almost impossible to destroy computer networks used by the armies without causing harm to civilian computer networks. Equally, there are challenges of establishing the taking of direct part in hostilities for civilians. These arise especially from the requirement of proving the presence of belligerent nexus, that is, a participating civilian intended to help a party to an armed conflict to the detriment of the other party.[67] Given the dual-use nature of some Information

---

62 Ibid.

63 See Ottis, R., *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, Cooperative Cyber Defence Centre of Excellence-Estonia, 2008.

64 See Rule 29 of the Hague Regulations, 1899.

65 See Dinstein, *The Principle of Distinction and Cyber War in International Armed Conflicts*, above note 49, at p. 34.

66 Greppi, *International Humanitarian Law in Cyber Operations, above note 59,* at p. 2.

67 Ibid, p. 27.

Technology (IT) facilities, some innocent civilians may find themselves indicted for cyber-attacks they know nothing about.[68]

Furthermore, the civilianization of armed conflicts causes a challenge to the applicability of IHL rules in incidences of cyber warfare.[69] Despite the IHL rules precluding civilians from taking direct part in hostilities,[70] their involvement in modern days conflicts has increased. They are used as operators of computer systems, acts as consultants, and provide expertise in ensuring that military activities are conducted successfully.[71] However, the emergence of cyber warfare has challenged the rules of IHL on civilian direct participation in hostilities in two ways:

First; IHL rules are only applied during armed conflict and within certain geographical limits.[72] In other words, the military confrontation between two or more parties to an armed conflict cannot be said to be the confrontation of the whole world. In that regard, cyber technology offers an opportunity for civilians to engage in cyber warfare while being stationed in conflict-neutral countries. In such circumstances, the traditional concept of civilian

---

68 Knopova, *New IHL Framework for Cyber Warfare*, above note 43, at p. 42.

69 Hathaway, O.A., *et al*, "The Law of Cyber-Attack", 100 (4) *California Law Review*, 2012, pp. 817-885, at p. 850.

70 Bosch, S., "The International Humanitarian Law Notion of Direct Participation in Hostilities-A Review of the ICRC Interpretive Guide and Subsequent Debata",17(3) *PELJ, 2014, pp. 1021-1022.*

71 Wenger A and Mason, SJA, "The civilianization of armed conflict: trends and implications" 90(872) *International Review of the Red Cross,* 2008, pp.835-852,at p. 842.

72 Delerue, F., "Civilian Direct Participation in Cyber Hostilities", 19 (1) *Derecho politica,* 2014, pp.3-17, at p. 5.

direct participation in hostilities which looks at the geographical limitation of armed conflict is under a serious challenge.[73]

Second; cyber warfare poses a practical challenge in establishing civilian's subjective intent in taking a direct part in hostilities. With the development of online platforms and the internet, persons can be attracted by lucrative offers to develop certain programmes or codes without knowing exactly how such codes or programmes are going to be used.[74] In such circumstances, civilians have found themselves engaging in military or cyber operations without having full knowledge of their actions. As a result, the establishment of criminal intent and ultimately prosecuting such civilians has always been difficult.[75]

What has been evident in this section is that, although the existing legal framework governing IHL can be applied to cyber warfare, the framework is not adequate. This is because cyber warfare has its unique features which, unfortunately, have not been adequately covered under the existing IHL rules.

4. THE LAW OF WAR TREATIES IN TANZANIA

For a long time now, rules of war have been used to limit the choice of the parties to an armed conflict to employ whatever means and methods during the confrontation.[76] The invocation of these rules aims at limiting the effects of war on mankind.[77] These

---

73 Ibid, p. 15.
74 Ibid.
75 Turns, D., "Cyber Warfare and the Notion of Direct Participation in Hostilities" 17 (2) *Journal of Conflict and Security Law*, 2012, pp. 279-297, at p. 288.
76 See Article 35 of Additional Protocol I.
77 Melzer, N., *International Humanitarian Law: A Comprehensive Introduction*, International Committee of the Red Cross, Geneva, 2019, at p. 17. See also

important rules are contained in the treaty law as well as in customary international law.[78] Ordinarily, they are meant to be applied on incidences of armed conflicts or state of a declared war.[79] Therefore, this subpart focuses on answering the question regarding the relevance of the law of war treaties to Tanzania, a country that has relatively enjoyed a long time of peaceful atmosphere since her independence in the 1960s. It also examines the Tanzanian legal regime with the intent to establish the extent to which the challenges of cyber warfare have been addressed.

5. THE RELEVANCE OF LAW OF WAR TREATIES IN TANZANIA

Unlike her neighbours in Eastern Africa and the Great Lakes Region, Tanzania has enjoyed and continues to enjoy a peaceful atmosphere within her territory. The existing peaceful atmosphere is argued to be one of the reasons for policymakers and legislators to think that treaty law containing IHL rules do not

---

Mack, M., *Increasing Respect for International Humanitarian Law in Non-International Armed Conflicts*, International Committee of the Red Cross, 2008, p. 5, available at https://www.icrc.org/sites/default/files/topic/file_plus_list/0923-increasing_respect_for_international_humanitarian_law_in_non-international_armed_conflicts.pdf (accessed 01 January 2020).

78 Liivoja, R., "Technological Change and the Evolution of the Law of War", 97(900) *International Review of the Red Cross*, 2015, pp. 1157-1177, at p. 1164.

79 See Article 2 common to all Four Geneva Conventions. See also Henckaerts, J., "Respect for the Convention" in Dormann, K., *et al* (eds), *Commentary on the First Geneva Convention: Convention (I) for the Amelioration ofthe Condition of the Wounded and Sick in Armed Forces in the Field*, Cambridge: Cambridge University Press, 2016, at p. 36. See also Ferraro, T., and Cameron, L., "Application of the Convention" in Dormann, K., *et al* (eds), *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, Cambridge : Cambridge University Press, 2016, at p. 68.

warrant heightened attention in Tanzania. Kamanga describes this attitude as a 'misguided perception'[80] clogging the minds of legislators and policymakers in the country. However, tracing the history of war in Tanzania, as well as assessing the country's situation, this article argues that deliberate efforts should be made to bring that perception to an end.

First, from 1978 to 1979 Tanzania was involved in an international armed conflict with Uganda under the fascist regime of Idi Amin.[81] The armed conflict between these two countries emanated, inter alia, from the invasion by Uganda's armed forces into the northern region of Tanzania (Kagera salient) in 1978.[82] In1972, not only Amin claimed Kagera salient to be part of Uganda but also sent his armed forces to reclaim the area.[83] However, this act of aggression did not result in the war due to the early intervention by the then Organization of African Unity (OAU) and the signing of the Mogadishu Agreement which obliged the two parties to respect the inherited colonial borders.[84] Before the implementation of the Mogadishu Agreement to the fullest, Idi Amin aggressively invaded the Kagera salient in 1978. This act was the turning point for the outbreak of war between Tanzania and Uganda which

---

80 Kamanga, K., "Implementation of International Humanitarian Law in Tanzania: A Legal Enquiry", in *African Yearbook on International Humanitarian Law*, Claremont: Juta and Company Ltd, 2012, at p. 41.

81 For more details on the fascist regime headed by Idi Amin in Uganda see Mamdani, M., "Imperialism and Fascism in Uganda: The Rise and Fall of Idi Amin", 18(38) *Economic and Political Weekly*, 1983, pp. 1614-1616, at p. 1614.

82 See Matata, C., "The Tanzanian-Ugandan War: Were the Just War Principles, Islamic Just War Tradition or the Catholic Ethics Followed?", 21(7) *Journal of Humanities and Social Sciences*, 2016, pp. 86-91, at p. 87.

83 See Roberts, G., "The Uganda-Tanzania War: The fall of Idi Amin, and the Failure of African Diplomacy, 1978-1979", 8(4) *Journal of Eastern African Studies*, 2014, pp. 692-709, at p. 695.

84 Ibid, at p. 693.

ended with the defeat and removal of Idi Amin's government from power.

The question of whether the war was fought in adherence to the law of war treaties is beyond the scope of this article. Suffice it to say that this armed conflict reveals that the country has an experience of war. This experience should remind policymakers of how relevant the rules of IHL are to Tanzania.

Secondly, Tanzanian troops have been involved in both peacekeeping and peace enforcement operations[85] in countries such as Lebanon, the Democratic Republic of Congo (DRC), Sudan, and Comoros.[86] In operations such as these, the relevance of IHL rules to Tanzania cannot be overemphasized. During peacekeeping operations, UN-mandated forces are required to be impartial and abstain from active combat except in self-defence cases. Similarly, peace enforcement operations require them to take sides and engage in active combat.[87] In the circumstances of either self-defence or engagement in active

---

85 On the difference between 'peace keeping' and 'peace enforcement' see Findlay, T., *The Use of Force in UN Peace Operations*, Oxford: SIPRI – Oxford University Press, 2002, at pp. 4-6.

86 See United Nations, "Service and Sacrifice: Tanzania Unwavering Commitment to UN Peacekeeping", UN News-Global Perspectives, available at https://news.un.org/en/gallery/526191 (accessed 05 January 2020). See also United Nations information Centre, *Tanzania Lost UN Peacekeepers on 7th December 2017*, available at https://unictz.org/2017/12/22/tanzania-lost-un-peacekeepers-on-7th-december-2017/ (accessed 05 January 2020).

87 Zwaneburg, M., 'Substantial Relevance of the Law of Occupation for Peace Operations' in Beruto, G.C, (Ed), *International Humanitarian Law, Human Rights and Peace Operations,* Geneva: ICRC, 2008, p. 158.

combat, UN-mandated forces are supposed to strictly abide by the rules of IHL.[88]

Thirdly, the peaceful atmosphere in Tanzania cannot and should not be used as a leeway towards putting less emphasis on the rules of IHL. Although the rules of IHL are applicable during armed conflict, treaty law obliges state parties to take 'certain measures' to ensure the implementation of IHL during 'peace times'.[89] This means that the obligations to implement certain measures under the law of war are to be done during peaceful times. This includes, among other things, the enactment of legislation to ensure IHL rules and their violations are taken care of under the domestic legal framework. For instance, the bomb blasts in Mbagala in 2009[90] and Gongo la Mboto in 2011 in Tanzania[91] posed huge challenges not only to the country's disaster preparedness but also to its commitment to implementing 'peacetime' IHL measures.[92] The Mbagala explosion alone killed 26 people that are, six army officers and 20 civilians.[93] More than 600 people were left injured and 9,049 houses were destroyed.[94] Similarly, the

---

88 Ibid.

89 See Article 2 Common to all Four Geneva Conventions – (Geneva Convention I – Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forced in Field, 1949, Geneva Convention II – Convention for the Amelioration of the Conditions of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 1949, Geneva Convention III – Convention Relative to the Treatment of Prisoners of War, 1949 and lastly, Geneva Convention IV – Convention Relative to the Protection of Civilian Persons in Time of War, 1949).

90 See Messo, I.N., "Prevalence of Post-Traumatic Stress Disorder in Children: The Case of the Mbagala Bomb Blasts in Tanzania", 18(5) *Journal of Health Psychology*, 2012, pp. 627-637, at p. 627.

91 Kamanga, *Implementation of International Humanitarian Law in Tanzania*, above note 72, at p. 44.

92 See Article 2 Common to all Four Geneva Conventions.

93 Messo, Prevalence of Post-Traumatic Stress Disorder in Children, above note 80, at p. 627.

94 Ibid.

Gongo la Mboto bomb blast killed 20 people; injured 200, and over 5,000 people both civilians and army officers were displaced from their homes.[95]

It is important to note that civilian casualties occurred due to the presence of civilian residences close to military camps. This shows that the principle of distinction under IHL which requires civilian objects to be distinguished from military objectives has received less attention in separating civilian residences from military camps. In effect, civilian casualties are expected to be high in all camps of this nature should there be a war between Tanzania and other States or non-state actors. Similarly, some military commanders may escape conviction for the loss of civilian lives and properties located close to such camps under the principles of proportionality and military necessity. It is, therefore, crucial that, Tanzania takes the necessary steps to remedy this situation.

6. THE RATIFICATION AND DOMESTICATION STATUS

Ratification and ultimately domestication of IHL treaties present another area where less attention has been given to the rules of war in Tanzania. With due regards to other sources of IHL,[96] the modern rules on the law of war are contained in the Four Geneva

---

[95] Mkinga, M., "Tanzania Explosions Leave the Public Deeply Skeptical", *The Citizen* (Dar es Salaam), 20 February 2011. See also Okwengo, N., "Tanzanian Families Reunited after Explosions", Report of the International Federation of Red Cross and Red Crescent Societies, 21 February 2011, available at https://reliefweb.int/report/united-republic-tanzania/tanzanian-families-reunited-after-explosions (accessed 6 January 2020).

[96] For the sources of IHL see Article 38 of the Statute of the International Court of Justice, 1946.

Conventions of 1949 and their three additional protocols of 1977.[97] Besides ratification, these rules require a domesticating act to become part and parcel of the laws of Tanzania. The *raison d'être* for this fact is the dualistic synergy between domestic laws and international treaties adopted by the constitution of the United Republic of Tanzania, 1977.[98] Under this arrangement, the Tanzanian parliament must enact enabling legislation to give the force of law to the ratified treaties in Tanzania.[99] Sadly, all the four Geneva Conventions and their three additional protocols have not been domesticated in Tanzania (See Table 1 below).

Table 1: Ratification/Domestication Status of IHL Instrument

SN	*Instrument's Name*	*Signature*	*Ratification /Accession*	*Domestication*
1.	Geneva Convention I		12.12.1962	Negative
2.	Geneva Convention II		12.12.1962	Negative
3.	Geneva		12.12.1962	Negative

[97] The three Additional Protocols are as follows: Additional Protocol I – Protocol Additional to the Geneva Conventions, 1949 Relating to the Protection of Victims of International Armed Conflict, 1977. Additional Protocol II – Protocol Additional to the Geneva Conventions, 1949 Relating to the Protection of Victims of Non-International Armed Conflicts, 1977 and Lastly, Additional Protocol III – Protocol Additional to the Geneva Conventions, 1949 Relating to the Adoption of an Additional Distinctive Emblem, 2005.

[98] See Article 63 (3) (d) and (e) of the Constitution of the United Republic of Tanzania, 1977. Also for a comprehensive understanding on the concepts of 'dualism' and 'monism' see Shyllon, O., "Monism/Dualism or Self Executory: The Application of Human Rights Treaties by Domestic Courts in Africa", *Institute for Human Rights*, Abo Akademi University, 2009, at p. 6.

[99] Kamanga, K., *Treaty Constipation' as a Critical Factor in Treaty Implementation: The Case of Kenya, Tanzania and Uganda*, Dar es Salaam: University of Dar es Salaam Repository, 2014, at p.3.

SN	*Instrument's Name*	*Signature*	*Ratification /Accession*	*Domestication*
	Convention III			
4.	Geneva Convention IV		12.12.1962	Negative
5.	Additional Protocol I		15.02.1983	Negative
6.	Additional Protocol II		15.02.1983	Negative
.	Additional Protocol III	08.02.2005	Negative	Negative

Source: ICRC, IHL Database (2020).

Similarly, the same trend of not completing the domestication process is seen in other instruments relevant to IHL such as; the Optional Protocol on Involvement of Children in Armed Conflict of 2000 (signed 11.11.2004), the Geneva Protocol on Asphyxiating or Poisonous Gases, and of Bacteriological Methods of 1925 (ratified 22.04.1963), Anti-Personnel Mine Ban Convention of 1997 (ratified 13.11.2000), the Convention on Cluster Munitions of 2008 (ratified 03.12.2008), the Convention Prohibiting Chemical Weapons of 1993 (ratified 25.06.1998), the Statute of International Criminal Court of 1998 (ratified 20.08.2002) and Treaty on Prohibition of Nuclear Weapons of 2017 (Signed 29.09.2019).[100]

[100] See ICRC, Treaties, States Parties and Commentaries Database – (Updated 2020) available at https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountrySelected.xsp?xp_countrySelected=TZ (accessed 7 January 2020).

Normally, the signing of a treaty imposes a duty to a signatory State to observe the principle of *pactasuntservanda*.[101] This fundamental principle of international law entails that the rights and duties accrued from the treaty law must be performed in good faith.[102] It is argued in this article that the absence of domesticating acts for the IHL Treaties, to which Tanzania is a party, offends the principle of *pactasuntservanda* and inevitably, elevates criticisms as to the country's true commitment to international obligations. Tanzania lags in the domestication of IHL rules. Some of her East African neighbours such as Kenya and Uganda are a step ahead of her both in the domestication and establishment of effective prosecution machinery for breaches of IHL.[103]

7. CYBER WARFARE VIS-À-VIS TANZANIAN LEGAL REGIME

Cyber technology, its accompanied threats, and challenges are a world reality today. The gaps it has unveiled to the existing rules of IHL are apparent and cannot be underrated. As already divulged in this article, the international community as a whole has not yet managed to conclude a comprehensive legal framework in response to the challenges of cyber warfare. Equally, the national

---

[101] See Article 26 of the Vienna Convention on the Law of Treaties, 1969.

[102] See Lukashuk, I.I., "The Principle *Pacta Sunt Servanda* and the Nature of Obligation under International Law", 83(3) *The American Journal of International Law*, 1989, pp. 513-518, at p. 513. See also Mwanawina, I., "Regional Integration and Pacta Sunt Servanda: Reflections on South African Trans-Border Higher Education Policies", 19(1) *Potchefstroomse Elektroniese Regsblad*, 2016, pp. 1-30, at p. 1.

[103] In Uganda see the Geneva Conventions Act of 1964 as well as the case of Uganda vs Thomas kwoyelo alias Latoni, Constitutional Appeal No. 01 of 2012, Ugandan Supreme Court, 05; in Kenya see the Geneva Conventions Act of 1968 and the International Crimes Act No. 16 of 2008 which domesticates the Rome Statute of 1998.

legal regimes are most often dawdling in responding to new phenomena and threats. Therefore, this subpart focuses on the Tanzanian legal framework and its response to the challenges of cyber warfare.

Tanzania's statutory books do not contain any specific legislation on IHL. Nevertheless, this article takes note of the existence of 'The Geneva Conventions Act (Colonial Territories) Order in Council of 28th July 1959'.[104] This was colonial legislation which extended the application of the 'Geneva Conventions Act of 1957' United Kingdom legislation) to colonies, including Tanganyika.[105] After its independence in 1961, the government of Tanganyika eschewed the international obligation on IHL extended to it by the colonial government.[106] This was done by ratifying all the four Geneva Conventions on the 12th December 1962. Even if the Geneva Conventions Act (Colonial Territories) Order in Council was to be considered law in Tanzania, several shortcomings would have tainted its applicability. For example, being a law of 1959, it would have not contained new developments captured by Additional Protocols of 1977. Furthermore, it would have brought complications on the scope of its applicability in Tanzania.

The High Court for Zanzibar in the case of *Director of Public Prosecutions v. Abdallah Suleiman Mwinyi and six*

---

[104] This was the Colonial Act No. 1301 of 1959 which became operational in Tanganyika on 1st September, 1959.

[105] See Section 2 of the Geneva Conventions Act (Colonial Territories) Order in Council, 1959. See also the First Schedule to this Order on Territories to which the Act extends.

[106] For more details see the Nyerere Doctrine of State Succession in Turack, D.C., "International Law and the New States of Africa, by Yilma Makonnen", 8(2) *Maryland Journal of International Law*, 1984, pp. 303-305, at p. 305.

others[107]insisted that any legislation originating from the 'Union Parliament' does not automatically apply in Zanzibar. It should first be legislation on union matters,[108] second; it should state that it applies both in Mainland Tanzania and Tanzania Zanzibar, and third; it must be tabled before the House of Representative in Zanzibar. Since the order, originated from colonial rule and mentioned only Tanganyika, it would have brought complications as to its applicability in Zanzibar.[109]

With regards to cyber warfare, few selected pieces of domestic legislation are examined and their role in mitigating the absence of specific legislation on IHL is stated. These statutes include; the Cyber Crimes Act, 2015, the Electronic and Postal Communications Act, 2010, the Prevention of Terrorism Act, 2002, the Penal Code, 1945, the Tanzania Red Cross Society Act, 1962, the National Defence Act, 1966, the Mutual Assistance in Criminal Matters Act, 1991 and the National Security Act, 1970.

7.1 The Cybercrimes Act, 2015

This is principal legislation dealing with the criminalization of cyber-related offences. Its objectives include inter alia the provisions for investigation, collection, and use of electronic evidence linked with computer systems and information technologies.[110] The Act does not make express reference to the rules of IHL or the Geneva Conventions. However, it creates

[107] Criminal Case No. 7 of 2016 (Unreported).

[108] See the List of Union Matters between Tanzania Mainland and Tanzania Zanzibar on the First Schedule to the Constitution of the United Republic of Tanzania, 1977.

[109] The United Republic of Tanzania was formed out of the Union between Tanganyika and Zanzibar. Not all laws apply to the whole of the United Republic. Some do apply in only one part of the Union.

[110] See the long title of the Cybercrimes Act, 2015.

certain offences, which if committed during cyber warfare have the potential of violating the rules of IHL. These offences are illegal access to a computer system (section 4), illegal interception of non-public transmission or circumvention of protection measures to prevent access thereof (section 6), illegal data interference (section 7), data espionage-which normally involves taking advantage of the advancement in information technology to obtain protected data without authorization (section 8) and illegal system interference which means the deliberate meddling or hindering the functioning or the usage of a computer system (section 9). It is also an offence to possess a device such as a computer program designed intentionally for the commission of crimes (section 10). Computer viruses fall under this category[111] because they can be designed and used to disrupt computer systems belonging to other persons.[112]In cyber warfare, computer viruses can be instructed to destroy the enemy's computer systems connected to air traffic control, nuclear plants, financial services, and other related systems.[113]

Other offences under the Act, 2015 include the publication of false information through a computer system, production and spreading of xenophobic or racist materials or insults, and publishing the materials to justify or inciting the commission of genocide or

---

[111] For more details on computer viruses as computer programs see Cohen, F., "Computer Viruses: Theory and Experiments", 6(1) *Computer and Security*, 1987, pp. 22 – 35, at p. 22.

[112] Balthrop, *et al*, *Technological Networks and the Spread of Computer Viruses*, above note 42, at p. 527.

[113] See how the computer virus 'stuxnet' was used by the United States of America and Israel in 2009 against the Iranian Uranium Enrichment facility in Siroli, G.P., "Considerations on Cyber Domain as the New Worldwid Battlefield", 53 (2) *The International Spectator*, 2018, pp. 111-123, at p. 122.

crimes against humanity.[114] The Act provides the court in Tanzania with powers to try cyber offences regardless of the nationality of the accused person.[115] For these powers to be exercised, the cyber-attack must have occurred whole or in part within the territory of the United Republic of Tanzania or directed against the ship or aircraft registered in Tanzania. The court can also exercise these powers with regard to an accused person who is a national of Tanzania residing abroad. The only requirement is that the act or omission, from which this national is accused of, must as well be considered a crime in the country of residence.[116]

Despite the Act's rich provisions on several offences which would have amounted to war crimes if committed during cyber warfare, the truth remains that, the Act is neither an IHL legislation nor was it enacted to address the challenges of cyber warfare.

7.2 The Electronic and Postal Communications Act, 2010

This Act has been enacted specifically to regulate issues of electronic and postal communications in Tanzania.[117] The Act is neither an IHL nor does it refer to the Geneva Conventions and their Additional Protocols. However, the Act is of great relevance to matters connected with cyber threats and security. Of utmost importance the Act establishes "the National Computer Emergency Response Team – (CERT)" and tasks it with among other things, the responsibilities to coordinate the national-level responses to cyber security incidences and cooperate internationally with other entities dedicated to the management of

[114] See sections 16, 17, 18 and 19 of the Cybercrimes Act, 2015.
[115] Ibid, Section 30.
[116] Ibid.
[117] See the long title of the Electronic and Postal Communications Act, 2010.

cyber security incidents.[118] For orderly and proper management, CERT is designated as a unit within the structure of the Tanzania Communication Regulatory Authority (TCRA).[119] Despite this incredible creativity of establishing CERT to curb cyber security incidents in Tanzania, still, the reality of the Act being a non-IHL instrument remains. As a consequence, this Act still does not answer the challenges of cyber warfare connected to the rules of IHL.

7.3 The National Security Act, 1970

Just like other legislation in Tanzania, the National Security Act of 1970 is neither an IHL instrument nor does it make explicit reference to the Geneva Conventions and their additional protocols. The rationale for enacting this legislation was to put in place a law which would deal with issues of state security, espionage, sabotage, and other activities detrimental to the safety and interests of Tanzania.[120] Given the range of issues that are to be dealt with under the National Security Act, it is not difficult to appreciate its relevance to the rules of IHL and cyber operations. First; the legislation criminalizes acts of 'espionage and sabotage' and whoever is found guilty of these offences will be sentenced to suffer life imprisonment.[121] Under the rules of IHL, espionage is defined as the clandestine gathering of the enemy's information with the intent to communicate the same to the other party to the conflict. Generally, acts of espionage are prohibited and would

[118] Ibid, section 124. See also Regulation 6 of the Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2018.
[119] See Regulation 5 (1) of the Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2018 [GN. No. 60/2018]..
[120] See the long title to the National Security Act, 1970 [Cap. 47. R.E. 2002].
[121] Ibid, section 3 (d).

make combatants lose the prisoner of war (POW) status if captured.[122] Unlike espionage, sabotage means intentional destruction or damage of materials, works, or installations.[123] If done during armed conflicts it should purely be for military purposes. A combatant who engages in sabotage acts by using proper means and methods of warfare and targeting military objectives cannot lose POW status if captured by the other party to the conflict.[124]

The related meaning of the two terms is portrayed under the National Security Act in which any person who, with prejudicial intent to the safety or interests of Tanzania, damages, hinders, or interferes with the carrying out of necessary services[125] or collects information in any manner whatsoever for direct or indirect use of a foreign state or disaffected person[126] commits an offence of sabotage or espionage as the case may be.[127] The fact that this is not an IHL legislation, the terms 'espionage and sabotage' are employed not in the strict sense as the one applicable under the

---

[122] See Rule 107 of Customary International Humanitarian Law available at https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf (accessed 16 January 2020). See also Article 46 of the Protocol Additional to the Geneva Conventions of 1949 and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) of 1977.

[123] See ICRC, Saboteur: How does the Law Protect in War? available at https://casebook.icrc.org/glossary/saboteur (accessed 16January 2020).

[124] Ibid.

[125] Section 2 of the National Security Act, 1970 [Cap. 47. R.E. 2002] provides a list of necessary services to include inter alia fire services or brigade, sanitation services, health services, hospitals, supply or generation of electricity, supply or distribution of water, production and supply of food or fuel, transport services or systems, mining industries, airfield, ports and any other declared necessary services by the President of the United Republic of Tanzania through published notice in the Gazette.

[126] See section 2 of the National Security Act, 1970 [Cap. 47. R.E. 2002] which defines disaffected person as the person carrying out seditious activities.

[127] Ibid, section 3.

rules of war. They can however be invoked during armed conflict especially if committed by the enemy side.

Secondly, concerning cyber operations, the National Security Act becomes relevant especially when it insists that a person commit acts of espionage when '*in any manner whatsoever'* makes a record of or relating to anything that may or intended to be useful to the foreign power or disaffected person.[128] It is the position of this Article that the use of the phrase 'any manner whatsoever' includes information or records generated by employing cyber technology. It should however be noted that this provision would be relevant to IHL when committed by the enemy side in IAC situations.

Lastly, like any other legislation in Tanzania, the National Security Act has not adequately provided answers to the challenges brought by cyber technology as far as the rules of IHL are concerned.

7.4 The Prevention of Terrorism Act, 2002

The scourge of terrorism is not wholly estranged from the rules of IHL. Cuyckens and Paulussen tell us that most specific acts prohibited under IHL such as the killing of civilians or persons placed *hors de combat,* taking of hostages and intentional targeting of civilian objects would qualify as terrorist acts outside the context of armed conflict.[129] During an armed conflict, the rules

[128] Ibid, section 3 (b).

[129] Cuyckens, H., and Paulussen, C., "The Prosecution of Foreign Fighters in Western Europe: The Difficult Relationship between Counter-Terrorism and International Humanitarian Law", 24(3) *Journal of Conflict and Security Law*, 2019, pp. 537-565, at p. 544.

of IHL are very clear on acts of terrorism by designating them as grave breaches of IHL amounting to war crimes.[130] The specific rules prohibit 'acts or threats of violence the primary purpose of which is to spread terror among civilian population'.[131] They also include other acts of terror against persons who are not taking direct part in hostilities and are in the hands of their enemy during NIAC or IAC.[132] With the development of cyber technology a new platform for terrorists to strategize and implement their plans has emerged. Cyber technology has made it easy for terrorists to spread their propaganda through the web, simplified their communication, recruitment, training, and even selecting targets of attack.[133]

To deal with acts of terrorism, Tanzania enacted the Prevention of Terrorism Act in 2002. This legislation put in place comprehensive measures to address the challenges of terrorism in Tanzania.[134] Additionally, the legislation paved a way for Tanzania to cooperate with other countries in confronting acts of terrorism both in terms of investigation and exchange of suspects.[135] The jurisdiction to try offences of terrorism is exclusively vested in the High Court of Tanzania and the High Court for Zanzibar.[136] Section 4(3) (g) of

---

[130] McKeever, D., "International Humanitarian Law and Counter-Terrorism: Fundamental Values, Conflicting Obligations", 69(1) *International and Comparative Law Quarterly*, 2020, pp. 43-78, at p. 51.

[131] See Article 51 (2) of Additional Protocol I. See also Article 13 (2) of Additional Protocol II. See also Rule 2 of Customary International Humanitarian Law, available at https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule2 (accessed 17 January 2020).

[132] Article 33 of Geneva Convention-IV. See also Article 4 (2) (d) of Additional Protocol II.

[133] See Adkins, G., "Red Teaming the Read Team: Utilizing Cyber Espionage to Combat Terrorism", 6(3) *Journal of Strategic Security,* 2013, pp. 1-9, at p. 2.

[134] See the long title to the Prevention of Terrorism Act, 2002.

[135] Ibid, section 37.

[136] The Judiciary is not a Union Matter in the United Republic of Tanzania save for the Court of Appeal of Tanzania the result of which there is the High Court of

the Prevention of Terrorism Act is the most relevant provision in addressing issues of terrorism and cyber technology. The provision acknowledges that acts of terrorism constitute inter alia 'any act or threat of action which is designed or intended to disrupt any computer system, services directly linked to communication infrastructure, financial services, utilities, transportation or other essential infrastructure'.[137] These acts or omissions do not automatically qualify as acts of terrorism unless they are executed with 'terrorist intention'.[138]

Unfortunately, one searches in vain for the meaning of 'terrorist intention' in the legislation. It is, therefore, argued in this article that 'terrorist intention' should be interpreted within the accepted main purpose of terrorism which is to spread terror to the population through acts or threats of violence in pursuit of political or ideological motives.[139] Hence, any intent to spread terror to the population through threats or violent means in furtherance of a political or ideological goal should qualify as 'terrorist intent'. Pre-attack behaviours, expressions, or sympathizing with terrorist ideologies can be used as indicative factors to prove the presence of 'terrorist intent' by law enforcers.[140] The Netherlands has

---

Tanzania and the High Court of Zanzibar – See Article 4 (2) and Item 21 of the First Schedule on Union Matters to the Constitution of the United Republic of Tanzania, 1977.

[137] Ibid, section 4 (3) (g).

[138] Ibid, section 4 (2).

[139] OHCHR, Human Rights, Terrorism and Counter-terrorism, Office of the United Nations High Commissioner for Human Rights, Facts sheet No. 32, at p. 5, available at https://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf (accessed 19 January 2020). See also Gibbs, J.P., "Conceptualization of Terrorism", 54(3) *American Sociological Review*, 1989, pp. 329-340, at p. 330.

[140] Schuurman, B., and Eijkman, Q., *Indicators of Terrorist Intent and Capability: Tools for Threat Assessment, Dynamics of Asymmetric Conflict: Pathways toward*

successfully employed this approach by collecting online radical views of the 17 years old child and successfully charged him for conspiring violent attack with 'terrorist intent'.[141]

Even with this clear understanding, applying the rules of IHL to the war on terror continues to be a challenge in Tanzania and the entire world. This is because the term 'war' as used by States in the fight against terrorism does not have the same meaning as the one provided for under the law of armed conflict. Similarly, one cannot say with certainty that the fight against terrorism by the government of Tanzania as defined in the Prevention of Terrorism Act, 2002 is equivalent to the involvement of Tanzania in armed conflict as illustrated under the Four Geneva Conventions and their Additional Protocols. Therefore, the Prevention of Terrorism Act, 2002 is not an IHL instrument and does not adequately address the challenges of cyber technology relative to the rules of IHL.

7.5 The Mutual Assistance in Criminal Matters Act, 1991

The crimes committed in cyberspace do not respect the national borders. Given the possibility of the criminals to use servers located in multiple countries, it is pertinent for countries to co-operate in locating and identifying suspects or witnesses,

---

Terrorism and Genocide, The Hague: Routledge – Tailor & Francis Group, 2015, at p. 1.

[141] In 2004, Yehya, the 17 years old child had planned to bomb the Israel Embassy, the office of the Dutch National Security Institute, harm non-Muslims and Dutch politicians who had a negative stance on Islam. He spread his radical views via an online platform. Using his online posts, he was successfully charged before the court for conspiring a violent attack with 'terrorist intent'. For more details on this case see Versteegt, I., *et al, Terrorism, Adversity and Identity: A Qualitative Study of Detained Terrorism Suspects in Comparison to other Detainees*, Amsterdam: NSCR, 2018, at p. 95, available at https://www.njb.nl/Uploads/2018/12/NSCR-Rapport-Terrorism-adversity-and-identity-181218.pdf (accessed 19 January 2020).

conducting investigations, and obtaining crucial pieces of evidence.[142] These important activities are achievable through the Mutual Assistance in Criminal Matters Act, 1991. The Act expressly enables Tanzania to cooperate with Commonwealth and other foreign countries for all matters connected with mutual assistance in criminal matters.[143] Under section 4 of the Act, the phrase "mutual assistance in criminal matters" is interpreted to include:

> the obtaining of evidence, documents or other Articles, the provision of documents and other records, the location and identification of witnesses or suspects, the execution of requests for search and seizure, the making of arrangements for persons to give evidence or assist in investigations, the forfeiture or confiscation of property in respect of offences …[144]

Although the Act does not explicitly mention the rules of IHL or the Geneva Conventions, it is easy to appreciate its value in the prosecution of cross-border crimes connected to cyber warfare and IHL. The only setback that continues to hinder Tanzania is the absence of domesticating Acts for the Rome Statute of the International Criminal Court, the Geneva Conventions and their Additional Protocols. Such a deficiency denies Tanzania an opportunity to effectively prosecute designated crimes under the said instruments.

---

142 Section 4 of the Mutual Assistance in Criminal Matters Act, 1991.
143 Ibid, see the long title to the Act.
144 Ibid, section 4.

7.6 The Tanzania Red Cross Society Act, 1962

At its inception, this Act was known as 'the Tanganyika Red Cross Society Act' of 1962. It established the Tanganyika Red Cross Society (TRCS) which existed as a branch of the British Red Cross Society until the 8th of August 1963 when ICRC recognized it as a 'national society' for Tanganyika.[145] On 28th August 1963, TRCS was admitted as a member of the International Federation of the Red Cross and Red Crescent Societies (IFRS).[146] The scope of applicability of the Act in 1963 was confined within the territory of Tanganyika. After the Union of Tanganyika and Zanzibar in 1964, neither its scope nor the name of the Act was changed. Thus, de jure the legislation was not applicable in Zanzibar but de facto the activities of TRCS extended to Zanzibar.

Ordinarily, the legal basis and source of inspiration for the Acts establishing 'National Societies' of this kind, are the Geneva Conventions, their Additional Protocols, and the Seven (7) Fundamental Principles of the Red Cross.[147] Surprisingly, the Tanganyika Red Cross Society Act did not make any reference to the aforementioned instrument or the fundamental principles of the Red Cross. However, on 19th September 2019 the Tanganyika Red Cross Society Act 1962 was amended and its name changed to Tanzania Red Cross Society Act of 1962.[148] The amendment not only renamed the society into Tanzania Red Cross Society but also settle the legal dilemma regarding the scope of applicability of

---

[145] Kamanga, *Implementation of International Humanitarian Law in Tanzania*, above note 72, at p. 55.

[146] Ibid.

[147] See ICRC, The Fundamental Principles of the Red Cross and the Red Crescent, available at https://www.icrc.org/en/doc/assets/files/other/icrc_002_0513.pdf (accessed 23 January 2020). These principles include: Humanity, Impartiality, Neutrality, Independence, Unity, Universality and Voluntary Service.

[148] See Section 47 of the Written Laws (Miscellaneous Amendments) Act, No. 4 of 2019.

the legislation. It stipulates that the act shall apply to both Mainland Tanzania and Tanzania Zanzibar.[149]

With these amendments, the Act makes direct reference to the Geneva Conventions, their Additional Protocols and declaring TRCS to be the 'Sole National Red Cross Society for the United Republic of Tanzania and a member of the International Federation of the Red Cross and Red Crescent Societies'.[150] Additionally, the amendment ensures that there will be no misuse of emblems, be it 'red cross or red crescent signs'.[151] It is insisted that emblems should be employed as an indicative sign that persons and equipment using them fall under the protection of the Geneva Conventions and their additional protocols.[152] It is an offence punishable by a jail term or fine for any person to use emblems fraudulently with intent to deceive other people.[153] During armed conflict or war, TRCS is authorized to furnish aid to the sick, wounded members of the armies, civilians, Prisoners of War (POWs), and other non-belligerents affected by war.[154]

Since the Tanzania Red Cross Society Act of 1962 makes direct reference to the Geneva Conventions and their Additional Protocols; it is not difficult to appreciate its value in so far as cyber warfare is concerned. Any cyber-attack during an armed conflict directed towards computer facilities of the Red Cross or Red

---

149 Ibid, Section 48.
150 Ibid, Sections 49 and 50.
151 Ibid, see Section 49 which interprets the term 'emblem' to mean Red Cross or the Red Crescent.
152 Ibid, section 52. See also section 49 in which the term 'Conventions' is interpreted to mean the Four Geneva Conventions and their Additional Protocols.
153 Ibid, section 51.
154 See Section 4 (1) (a) of the Tanzania Red Cross Society Act, 1962.

crescent movement will amount to a violation of the Tanzania Red Cross Society Act as well as the Geneva Conventions and their Additional Protocols.

7.7 The Penal Code, 1945 and the National Defence Act, 1966

Generally, captured combatants in IAC are entitled to POW status.[155] The Penal Code and the National Defence Act are the two major pieces of legislation that address the question of POWs in Tanzania. Under Penal Code, any person who aids a POW to escape from a place of confinement commits an offence punishable by life imprisonment.[156] It goes without saying that aiding POWs who were involved in cyber-attacks before being captured by Tanzania People's Defence Force (TPDF) would amount to an offence under this provision.

The National Defence Act on the other side concentrates more on the duties of TPDF members who have fallen in the hands of the enemy as POWs.[157] It makes it an offence for any TPDF member to be captured and made a POW due to failure to exercise due precaution or disobedience of orders or willful neglect of duty. TPDF members who are POWs are prohibited from aiding, serving, or cooperating with the armed forces of the enemy while in custody. Additionally, the Act insists that a POW who prevents or discourages other members from escaping or rejoining the Tanzanian army commits an offence. These offences if committed

---

[155] Article 4 of Geneva Convention III.
[156] See Section 48 of the Penal Code, 1945 [Cap. 16. R.E. 2002].
[157] See Rule C.14 of the First Schedule to the National Defence Act, 1966 [Cap. 192. R.E. 2002].

traitorously do attract the death penalty, and in any other case, life imprisonment or a lesser punishment.[158]

Unlike Geneva Convention III, the National Defence Act focuses more on regulating members of the TPDF while putting less emphasis on POWs from enemy States. The Act incriminates any POW who escapes or attempts to escape from any lawful confinement in Tanzania.[159] This goes against the provisions of Geneva Convention III, which Tanzania has acceded since 1962. Under this Convention, it is not a criminal offence for POWs to escape or even attempt to escape from custody.[160] POWs who have unsuccessfully attempted to escape can only be subjected to disciplinary punishment even if it is a repeated offence.[161]

Lastly, the two pieces of legislation are neither IHL instruments nor do they make direct reference to the Geneva Conventions and their additional protocols. However, one may still appreciate their link with the rules of IHL and cyber warfare in as much as the question of POW is concerned.

8. REPRESSING IHL VIOLATIONS VIA ORDINARY CRIMES APPROACH

As already noted, Tanzania has not domesticated all the four Geneva Conventions and their Additional Protocols. This has denied Tanzania an opportunity to have an effective domestic mechanism to repress the violations of IHL. However, it is

158 Ibid.
159 Ibid, Rule C.38.
160 See Article 91 of Geneva Convention III.
161 Ibid, Article 92.

accepted that countries with no domestic legal mechanism to prosecute war crimes, may resort to ordinary crimes approach as an alternative.[162] This means that Tanzania may prosecute war crimes as domestic 'ordinary' crimes under her penal laws. The basis for this approach is rooted in Article 17 (1) (a) of the Rome Statute of the International Criminal Court, 1998 which insists on the prosecution of international crimes at domestic courts provided that States are 'willing and able' to do so. Scholars reveal that the interpretation of this provision emphasizes 'conducts' rather than 'legal characterization'.[163] In other words, if murder has been committed or rape has occurred during an armed conflict, States with no mechanism to handle these crimes as war crimes may still prosecute them as ordinary crimes under their legal framework.[164] Nevertheless, the prosecution of war crimes as ordinary crimes can only be accepted if the aim and its eventual outcome are to genuinely punish the perpetrators of crimes within the spirit of the international criminal and humanitarian instruments.[165]

Since there is no domestic mechanism to repress war crimes in Tanzania, the ordinary crimes approach appears to be the option at hand. This entails that the loss of lives or properties of protected persons due to cyber warfare may be sanctioned as 'ordinary crimes' under the Tanzanian legal regime. Despite this

---

[162] Kweka, G.J., "International Criminal Justice at Domestic Level in Kenya: Reality on the Ground", 42 (2) *Eastern Africa Law Review*, 2015, pp. 84-111, at p. 91.

[163] Lubaale, E.C., "Limitations of the Ordinary-Crimes Approach to the International Crime of Rape: The Case of Uganda", 12 (1) *African Journal of Legal Studies*, 2020, pp. 266-297, p. 268. See also Batros, B., "The Evolution of the ICC Jurisprudence on Admissibility", in Stahn, C., and El Zeidy, M., (eds), *The International Criminal Court and Complementarity*, New York: Cambridge University Press, 2011, at p. 75.

[164] Materu, S.F., *The Post-Election Violence in Kenya: Domestic and International Legal Responses,* The Hague: T.M.C Asser Press, 2015, at p. 93.

[165] Ibid.

possibility, the ordinary crimes approach still faces several pitfalls and cannot adequately be the solution to the challenges brought by cyber warfare. Among these pitfalls include the differences in defences available for war crimes and ordinary crimes. For instance; perpetrators of cyber-attack on a civil and military air traffic control system which led to the crash of the civilian aircraft may rely on the principles of military necessity or proportionality to exonerate themselves from criminal liability. Nonetheless, under the Tanzanian legal framework, perpetrators who caused deaths to other persons may raise defences such as provocation, self-defence, or defence to the life of another person.[166] All defences other than those embedded within the domestic penal laws cannot be entertained by the Tanzanian Courts. Therefore, prosecuting war crimes as ordinary crimes within the Tanzanian legal framework has the risk of leading to wrongful convictions of persons who otherwise have proper defences under the rules of IHL.

The absence of crimes that correspond or are equivalent to war crimes in the Tanzanian legal regime is another pitfall. For example, forcing protected persons or POWs to serve in the enemy's forces is not recognized as a crime under the domestic legal framework in Tanzania.[167] In this circumstance, the prosecution of a war crime as an 'ordinary' crime falls short of practical realities. This is as well captured within the principle of legality which prohibits the prosecution of persons for crimes that are not prescribed in the law or punishing individuals for non-

[166] See Chapter IV of the Penal Code, 1945 (Tanzania).

[167] For the detailed explanation of this challenge regarding the Ugandan penal laws see Lubaale, *Limitations of the Ordinary-Crimes Approach to the International Crime of Rape,* above note 2, at p. 276.

existent crimes.[168] Hence, perpetrators of war crimes may end-up being acquitted for the crimes committed in the context of armed conflict, simply because such crimes or their equivalent are not contained in the Tanzanian legal framework.

Although Tanzania may resort to an ordinary crime approach to suppress IHL violations, the approach inadequately provides answers to the challenges brought by cyber technology to the rules of IHL. To address the shortcomings of applying the ordinary crimes approach to war crimes, Tanzania is left with no option but to take serious legislative steps of enacting specific laws that domesticate IHL rules and address the challenges of cyber warfare.

9. CONCLUDING REMARKS

This article has focused on examining the law of armed conflict in an era of cyber technology. Specifically, the article highlighted the challenges of cyber warfare to the rules of IHL and domestic response by Tanzania. The article insists that the presence of cyber technology both as means and methods of warfare in today's world is a reality which must be confronted. It shows that the existing rules of IHL have a limited application to the incidences of cyber warfare. In depicting those limitations, the article identifies and explains several unique features of cyber warfare which are not addressed by the contemporary rules of IHL.

---

[168] For more details on the principle of legality in criminal law see Barzegarzadeh, A., Karveh, M.J., and Raisi, L., "Principle of Legality and its Relation with Customary Law in International Criminal Law", 6 (5) *Mediterranean Journal of Social Sciences*, 2015, pp. 398-402, at p. 400.

Additionally, the article examined the domestic legal framework in Tanzania, its synergy with the rules of IHL, and how it has responded to the challenges of cyber warfare. The Article reveals that Tanzania has paid less attention to the rules of IHL. This is reflected in the way Tanzania has implemented her IHL obligations during peaceful times. First: there have been incidences where civilian residences have been constructed close to military camps. This seriously hit into the IHL rules which require the distinction to be made between civilian objects and military objectives in as far as 'peace-time' measures are concerned. Secondly, being a dualist state, it was expected that after ratification, Tanzania would have moved a step further to domesticate the Geneva Conventions, their Additional Protocols, and other instruments relevant to IHL. However, this has not been the case, as a result, Tanzania does not have an effective domestic mechanism to repress IHL violations.

Since Tanzania has not domesticated IHL instruments, the Article discussed her chances of resorting to an 'ordinary crimes approach' as a repressive mechanism for IHL violations. Although this approach can be invoked by Tanzania, its application is tainted with several legal and practical challenges. Such challenges may either lead to wrongful convictions or acquittals of perpetrators of war crimes. The Article also links the ordinary crimes approach to the violations of IHL rules during cyber warfare and concludes that the approach does not adequately provide answers to the challenges introduced by cyber technology to the rules of IHL.

The Article further examined legal provisions scattered in various pieces of legislation in Tanzania. It sought to identify the relevance of such provisions to the IHL rules and their responses to the challenges of cyber warfare. The Article found out that apart from the Tanzania Red Cross Society Act, 1962, all other discussed pieces of legislation did not make direct reference to the Geneva Conventions or their Additional Protocols. This meant that such pieces of legislation were not meant to address the questions relating to the rules of IHL. Although few provisions in those pieces of legislation are relevant to the IHL rules, they still do not provide a cure to the challenges brought by cyber warfare.

Basing on the arguments made in this article, the following recommendations are made:

First, Tanzania should domesticate IHL treaties and ensure that the domesticating Act contains provisions which provide answers to the challenges of cyber warfare. Since the challenges of cyber technology to the rules of IHL are known, Tanzania cannot and should not shy away from addressing them. It is, therefore, important that Tanzania execute her IHL obligations by implementing IHL peace-time measures which include domesticating IHL treaties and providing answers to the puzzle caused by the emergence of cyber technology.

Second, Tanzania should ensure that the National Defence Act, 1966 is amended. The amendment should aim at removing the existing inconsistency between the Act and the Geneva Convention Relative to the Treatment of the POWs. As it stands, the National Defence Act, incriminate POWs who escape or attempt to escape from lawful custody in Tanzania. This is entirely

contrary to the rules of IHL provided for under the Geneva Convention III to which Tanzania is a party.

Third, necessary legal and administrative steps should be taken by the government of Tanzania to restrict civilians from constructing their residences close to military camps. The development of towns and cities in Tanzania has increased the demand for residential lands in urban areas. With more demands, Tanzania has witnessed the mushrooming of civilian residences close to military camps. The Mbagala and Gongo la Mboto bomb blasts only served as a reminder of how dangerous it is for civilians to build their houses close to military objects. If this trend is not controlled, civilian casualties cannot be avoided during an armed conflict between Tanzania and other States or non-state actors.